

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problems Mailbox.**

**THIS PAGE BLANK (USPTO)**

09/ 5650  
869434

**TRAITE DE COOPERATION EN MATIERE DE BREVETS**

**PCT****NOTIFICATION CONCERNANT LA  
TRANSMISSION DE DOCUMENTS**

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Commissioner  
US Department of Commerce  
United States Patent and Trademark  
Office, PCT  
2011 South Clark Place Room  
CP2/5C24  
Arlington, VA 22202  
ETATS-UNIS D'AMERIQUE  
en sa qualité d'office désigné

Date d'expédition (jour/mois/année)

19 juillet 2001 (19.07.01)

Demande internationale no

PCT/FR99/02979

Date du dépôt international

01 décembre 1999 (01.12.99)

Déposant

COMMISSARIAT A L'ENERGIE ATOMIQUE etc

**RECEIVED**

OCT 01 2001

Technology Center 2100

Le Bureau international transmet ci-joint le nombre de copies indiqué ci-après des documents suivants:

\_\_\_\_\_ copie(s) du (des) document(s) de priorité (règle 17.2.a))

**CORRECTED  
VERSION**

Bureau international de l'OMPI  
34, chemin des Colombettes  
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

Jocelyne Rey-Millet

no de téléphone: (41-22) 338.83.38

**THIS PAGE BLANK (USPTO)**

PCT

REQUÊTE

Le soussigné requiert que la présente demande internationale soit traitée conformément aux dispositions énumérées de brevets.

Réservé à l'office récepteur

Demande internationale n°

Date du dépôt international

Nom de l'office récepteur et "Demande internationale PCT"

Référence du dossier du déposant ou du mandataire (facultatif)  
(12 caractères au maximum) PCT 3855/BC

Cadre n° I TITRE DE L'INVENTION

Terminal sécurisé muni d'un lecteur de carte à puce destiné à communiquer avec un serveur via un réseau de type internet.

Cadre n° II DÉPOSANT

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)

BULL CP8  
68, route de Versailles  
BP 45  
78430 LOUVECIENNES  
FRANCE

☐ Cette personne est aussi inventeur.

n° de téléphone  
(33) 1 39.66.61.76

n° de télécopieur  
(33) 1 39.66.61.73

n° de téléimprimeur

Nationalité (nom de l'Etat) : FRANCE

Domicile (nom de l'Etat) : FRANCE

Cette personne est déposant pour : ☐ tous les Etats désignés ☒ tous les Etats désignés sauf les Etats-Unis d'Amérique ☐ les Etats-Unis d'Amérique ☐ les Etats indiqués dans le cadre supplémentaire

Cadre n° III AUTRE(S) DÉPOSANT(S) OU (AUTRE(S)) INVENTEUR(S)

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)

MARIANA Renaud  
5 Square Las Cases  
78150 LE CHESNAY  
FRANCE

Cette personne est :

☐ déposant seulement  
☒ déposant et inventeur  
☐ inventeur seulement  
(Si cette case est cochée, ne pas remplir la suite.)

Nationalité (nom de l'Etat) : FRANCE

Domicile (nom de l'Etat) : FRANCE

Cette personne est déposant pour : ☐ tous les Etats désignés ☐ tous les Etats désignés sauf les Etats-Unis d'Amérique ☒ les Etats-Unis d'Amérique ☐ les Etats indiqués dans le cadre supplémentaire

☐ D'autres déposants ou inventeurs sont indiqués sur une feuille annexe.

Cadre n° IV MANDATAIRE OU REPRÉSENTANT COMMUN; OU ADRESSE POUR LA CORRESPONDANCE

La personne dont l'identité est donnée ci-dessous est/a été désignée pour agir au nom du ou des déposants auprès des autorités internationales compétentes, comme : ☒ mandataire ☐ représentant commun

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays.)

BULL S.A  
CORLU Bernard  
PC58D20 / 68, route de Versailles  
F- 78434 LOUVECIENNES Cedex (FRANCE)

n° de téléphone  
(33) 1 39.66.61.76

n° de télécopieur  
(33) 1 39.66.61.73

n° de téléimprimeur

☐ Adresse pour la correspondance : cocher cette case lorsque aucun mandataire ni représentant commun n'est/n'a été désigné et que l'espace ci-dessus est utilisé pour indiquer une adresse spéciale à laquelle la correspondance doit être envoyée.

**THIS PAGE BLANK (USPTO)**

## Cadre n° V DÉSIGNATION D'ÉTATS

Les désignations suivantes sont faites conformément à la règle 4.9.a) (cocher les cases appropriées; une au moins doit l'être) :

## Brevet régional

- ☐ AP Brevet ARIPO : GH Ghana, GM Gambie, KE Kenya, LS Lesotho, MW Malawi, SD Soudan, SL Sierra Leone, SZ Swaziland, TZ République-Unie de Tanzanie, UG Ouganda, ZW Zimbabwe et tout autre État qui est un État contractant du Protocole de Harare et du PCT
- ☐ EA Brevet eurasien : AM Arménie, AZ Azerbaïdjan, BY Bélarus, KG Kirghizistan, KZ Kazakhstan, MD République de Moldova, RU Fédération de Russie, TJ Tadjikistan, TM Turkménistan et tout autre État qui est un État contractant de la Convention sur le brevet eurasien et du PCT
- ☒ EP Brevet européen : AT Autriche, BE Belgique, CH et LI Suisse et Liechtenstein, CY Chypre, DE Allemagne, DK Danemark, ES Espagne, FI Finlande, FR France, GB Royaume-Uni, GR Grèce, IE Irlande, IT Italie, LU Luxembourg, MC Monaco, NL Pays-Bas, PT Portugal, SE Suède et tout autre État qui est un État contractant de la Convention sur le brevet européen et du PCT
- ☐ OA Brevet OAPI : BF Burkina Faso, BJ Bénin, CF République centrafricaine, CG Congo, CI Côte d'Ivoire, CM Cameroun, GA Gabon, GN Guinée, GW Guinée-Bissau, ML Mali, MR Mauritanie, NE Niger, SN Sénégal, TD Tchad, TG Togo et tout autre État qui est un État membre de l'OAPI et un État contractant du PCT (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée) . . . . .

## Brevet national (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée) :

- |  |   |
|--|---|
| <input type="checkbox"/> AE Émirats arabes unis                        | <input type="checkbox"/> LR Liberia                               |
| <input type="checkbox"/> AL Albanie                                    | <input type="checkbox"/> LS Lesotho                               |
| <input type="checkbox"/> AM Arménie                                    | <input type="checkbox"/> LT Lituane                               |
| <input type="checkbox"/> AT Autriche                                   | <input type="checkbox"/> LU Luxembourg                            |
| <input checked="" type="checkbox"/> AU Australie                       | <input type="checkbox"/> LV Lettonie                              |
| <input type="checkbox"/> AZ Azerbaïdjan                                | <input type="checkbox"/> MA Maroc                                 |
| <input type="checkbox"/> BA Bosnie-Herzégovine                         | <input type="checkbox"/> MD République de Moldova                 |
| <input type="checkbox"/> BB Barbade                                    | <input type="checkbox"/> MG Madagascar                            |
| <input type="checkbox"/> BG Bulgarie                                   | <input type="checkbox"/> MK Ex-République yougoslave de Macédoine |
| <input type="checkbox"/> BR Brésil                                     |   |
| <input type="checkbox"/> BY Bélarus                                    | <input type="checkbox"/> MN Mongolie                              |
| <input type="checkbox"/> CA Canada                                     | <input type="checkbox"/> MW Malawi                                |
| <input type="checkbox"/> CH et LI Suisse et Liechtenstein              | <input type="checkbox"/> MX Mexique                               |
| <input checked="" type="checkbox"/> CN Chine                           | <input type="checkbox"/> NO Norvège                               |
| <input type="checkbox"/> CR Costa Rica                                 | <input type="checkbox"/> NZ Nouvelle-Zélande                      |
| <input type="checkbox"/> CU Cuba                                       | <input type="checkbox"/> PL Pologne                               |
| <input type="checkbox"/> CZ République tchèque                         | <input type="checkbox"/> PT Portugal                              |
| <input type="checkbox"/> DE Allemagne                                  | <input type="checkbox"/> RO Roumanie                              |
| <input type="checkbox"/> DK Danemark                                   | <input type="checkbox"/> RU Fédération de Russie                  |
| <input type="checkbox"/> DM Dominique                                  | <input type="checkbox"/> SD Soudan                                |
| <input type="checkbox"/> EE Estonie                                    | <input type="checkbox"/> SE Suède                                 |
| <input type="checkbox"/> ES Espagne                                    | <input checked="" type="checkbox"/> SG Singapour                  |
| <input type="checkbox"/> FI Finlande                                   | <input type="checkbox"/> SI Slovénie                              |
| <input type="checkbox"/> GB Royaume-Uni                                | <input type="checkbox"/> SK Slovaquie                             |
| <input type="checkbox"/> GD Grenade                                    | <input type="checkbox"/> SL Sierra Leone                          |
| <input type="checkbox"/> GE Géorgie                                    | <input type="checkbox"/> TJ Tadjikistan                           |
| <input type="checkbox"/> GH Ghana                                      | <input type="checkbox"/> TM Turkménistan                          |
| <input type="checkbox"/> GM Gambie                                     | <input type="checkbox"/> TR Turquie                               |
| <input type="checkbox"/> HR Croatie                                    | <input type="checkbox"/> TT Trinité-et-Tobago                     |
| <input type="checkbox"/> HU Hongrie                                    | <input type="checkbox"/> TZ République-Unie de Tanzanie           |
| <input type="checkbox"/> ID Indonésie                                  | <input type="checkbox"/> UA Ukraine                               |
| <input type="checkbox"/> IL Israël                                     | <input type="checkbox"/> UG Ouganda                               |
| <input type="checkbox"/> IN Inde                                       | <input checked="" type="checkbox"/> US États-Unis d'Amérique      |
| <input type="checkbox"/> IS Islande                                    |   |
| <input checked="" type="checkbox"/> JP Japon                           | <input type="checkbox"/> UZ Ouzbékistan                           |
| <input type="checkbox"/> KE Kenya                                      | <input type="checkbox"/> VN Viet Nam                              |
| <input type="checkbox"/> KG Kirghizistan                               | <input type="checkbox"/> YU Yougoslavie                           |
| <input type="checkbox"/> KP République populaire démocratique de Corée | <input type="checkbox"/> ZA Afrique du Sud                        |
| <input checked="" type="checkbox"/> KR République de Corée             | <input type="checkbox"/> ZW Zimbabwe                              |
| <input type="checkbox"/> KZ Kazakhstan                                 |   |
| <input type="checkbox"/> LC Sainte-Lucie                               |   |
| <input type="checkbox"/> LK Sri Lanka                                  |   |

Cases réservées pour la désignation d'États qui sont devenus parties au PCT après la publication de la présente feuille :

- ☐ . . . . .
- ☐ . . . . .

Déclaration concernant les désignations de précaution : outre les désignations faites ci-dessus, le déposant fait aussi conformément à la règle 4.9.b) toutes les désignations qui seraient autorisées en vertu du PCT, à l'exception de toute désignation indiquée dans le cadre supplémentaire comme étant exclue de la portée de cette déclaration. Le déposant déclare que ces désignations additionnelles sont faites sous réserve de confirmation et que toute désignation qui n'est pas confirmée avant l'expiration d'un délai de 15 mois à compter de la date de priorité doit être considérée comme retirée par le déposant à l'expiration de ce délai. (La confirmation (y compris les taxes) doit parvenir à l'office récepteur dans le délai de 15 mois.)

**THIS PAGE BLANK (USPTO)**



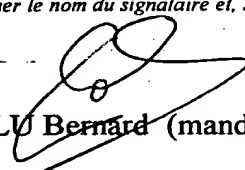
Cadre n° VI REVENDICATION DE PRIORITÉ		<input type="checkbox"/> D'autres revendications de priorité sont indiquées dans le cadre supplémentaire.		
Date de dépôt de la demande antérieure (jour/mois/année)	Numéro de la demande antérieure	Lorsque la demande antérieure est une :		
		demande nationale : pays	demande régionale :* office régional	demande internationale : office récepteur
(1) 28 octobre 1999 (28.10.1999)	99 13508	FRANCE		
(2)				
(3)				

☒ L'office récepteur est prié de préparer et de transmettre au Bureau international une copie certifiée conforme de la ou des demandes antérieures (seulement si la demande antérieure a été déposée auprès de l'office qui, aux fins de la présente demande internationale, est l'office récepteur) indiquées ci-dessus au(x) point(s) : 1

\* Si la demande antérieure est une demande ARIPO, il est obligatoire d'indiquer dans le cadre supplémentaire au moins un pays partie à la Convention de Paris pour la protection de la propriété industrielle pour lequel cette demande antérieure a été déposée (règle 4.10.b)ii). Voir le cadre supplémentaire.

Cadre n° VII ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE			
<b>Choix de l'administration chargée de la recherche internationale (ISA)</b> (si plusieurs administrations chargées de la recherche internationale sont compétentes pour procéder à la recherche internationale, indiquer l'administration choisie; le code à deux lettres peut être utilisé) : <b>ISA /</b>	<b>Demande d'utilisation des résultats d'une recherche antérieure; mention de cette recherche</b> (si une recherche antérieure a été effectuée par l'administration chargée de la recherche internationale ou demandée à cette dernière) : <div style="display: flex; justify-content: space-between;"> <div>Date (jour/mois/année) <b>28.10.99</b></div> <div>Numéro <b>99 13508 FA 577886</b></div> <div>Pays (ou office régional) <b>FR</b></div> </div>		

Cadre n° VIII BORDEREAU; LANGUE DE DÉPÔT	
La présente demande internationale contient le nombre de feuilles suivant :  requête : <b>03</b> description (sauf partie réservée au listage des séquences) : <b>31</b> revendications : <b>04</b> abrégé : <b>01</b> dessins : <b>04</b> partie de la description réservée au listage des séquences : _____  Nombre total de feuilles : <b>43</b>	Le ou les éléments cochés ci-après sont joints à la présente demande internationale : 1. <input type="checkbox"/> feuille de calcul des taxes 2. <input checked="" type="checkbox"/> pouvoir distinct signé 3. <input type="checkbox"/> copie du pouvoir général; numéro de référence, le cas échéant : 4. <input type="checkbox"/> explication de l'absence d'une signature 5. <input checked="" type="checkbox"/> document(s) de priorité indiqué(s) dans le cadre n° VI au(x) point(s) : <b>1</b> 6. <input type="checkbox"/> traduction de la demande internationale en (langue) : 7. <input type="checkbox"/> indications séparées concernant des micro-organismes ou autre matériel biologique déposés 8. <input type="checkbox"/> listage des séquences de nucléotides ou d'acides aminés sous forme déchiffrable par ordinateur 9. <input checked="" type="checkbox"/> autres éléments (préciser) : <b>Rapport de Recherche FA 577886</b>
Figure des dessins qui doit accompagner l'abrégé : <b>3</b>	Langue de dépôt de la demande internationale : <b>FRANCAIS</b>

Cadre n° IX SIGNATURE DU DÉPOSANT OU DU MANDATAIRE
À côté de chaque signature, indiquer le nom du signataire et, si cela n'apparaît pas clairement à la lecture de la requête, à quel titre l'intéressé signe.   <b>CORLU Bernard (mandataire)</b>

Réservé à l'office récepteur

1. Date effective de réception des pièces supposées constituer la demande internationale :  3. Date effective de réception, rectifiée en raison de la réception ultérieure, mais dans les délais, de documents ou de dessins complétant ce qui est supposé constituer la demande internationale :  4. Date de réception, dans les délais, des corrections demandées selon l'article 11.2) du PCT :	2. Dessins : <input type="checkbox"/> reçus :  <input type="checkbox"/> non reçus :
5. Administration chargée de la recherche internationale (si plusieurs sont compétentes) : <b>ISA /</b>	6. <input type="checkbox"/> Transmission de la copie de recherche différée jusqu'au paiement de la taxe de recherche.

Réservé au Bureau international

Date de réception de l'exemplaire original par le Bureau international :	
--	--

**THIS PAGE BLANK (USPTO)**

# TRAITÉ DE COOPERATION EN MATIERE DE BREVETS

PCT

## NOTIFICATION DE LA RECEPTION DE L'EXEMPLAIRE ORIGINAL

(règle 24.2.a) du PCT)

**PTO/PCT Rec'd 28 JUN 2001**

Expéditeur: le BUREAU INTERNATIONAL

Propriété Intellectuelle

Destinataire:

18 DEC. 2000

**BULL S.A.**

CORLU, Bernard  
Bull S.A.  
PC58D20  
68, route de Versailles  
F-78434 Louveciennes Cedex  
FRANCE

Date d'expédition (jour/mois/année) 23 novembre 2000 (23.11.00)	NOTIFICATION IMPORTANTE
Référence du dossier du déposant ou du mandataire PCT 3855/BC	Demande internationale no PCT/FR00/02979

Il est notifié au déposant que le Bureau international a reçu l'exemplaire original de la demande internationale précisée ci-après.

Nom(s) du ou des déposants et de l'Etat ou des Etats pour lesquels ils sont déposants:

**BULL CP8 (pour tous les Etats désignés sauf US)**

**MARIANA, Renaud (pour US seulement)**

Date du dépôt international	:	26 octobre 2000 (26.10.00)
Date(s) de priorité revendiquée(s)	:	28 octobre 1999 (28.10.99)
Date de réception de l'exemplaire original par le Bureau international	:	16 novembre 2000 (16.11.00)
Liste des offices désignés	:	

EP : AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE  
National : AU, CN, JP, KR, SG, US

### ATTENTION

Le déposant doit soigneusement vérifier les indications figurant dans la présente notification. En cas de divergence entre ces indications et celles que contient la demande internationale, il doit aviser immédiatement le Bureau international.

En outre, l'attention du déposant est appelée sur les renseignements donnés dans l'annexe en ce qui concerne

- ☒ les délais dans lesquels doit être abordée la phase nationale
- ☒ la confirmation des désignations faites par mesure de précaution
- ☒ les exigences relatives aux documents de priorité.

Une copie de la présente notification est envoyée à l'office récepteur et à l'administration chargée de la recherche internationale.

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse n° de télécopieur (41-22) 740.14.35	Fonctionnaire autorisé Yolaine CUSSAC n° de téléphone (41-22) 338.83.38
---	---

**THIS PAGE BLANK (USPTO)**

**RENSEIGNEMENTS CONCERNANT LES DELAIS DANS LESQUELS DOIT ETRE ABORDEE  
LA PHASE NATIONALE**

Il est rappelé au déposant qu'il doit aborder la "phase nationale" auprès de chacun des offices désignés indiqués sur la notification de la réception de l'exemplaire original (formulaire PCT/IB/301) en payant les taxes nationales et en remettant les traductions, telles qu'elles sont prescrites par les législations nationales.

Le délai d'accomplissement de ces actes de procédure est de **20 MOIS** à compter de la date de priorité ou, pour les Etats désignés qui ont été élus par le déposant dans une demande d'examen préliminaire international ou dans une élection ultérieure, de **30 MOIS** à compter de la date de priorité, à condition que cette élection ait été effectuée avant l'expiration du 19e mois à compter de la date de priorité. Certains offices désignés (ou élus) ont fixé des délais qui expirent au-delà de 20 ou 30 mois à compter de la date de priorité. D'autres offices accordent une prolongation des délais ou un délai de grâce, dans certains cas moyennant le paiement d'une taxe supplémentaire.

En plus de ces actes de procédure, le déposant devra dans certains cas satisfaire à d'autres exigences particulières applicables dans certains offices. **Il appartient au déposant** de veiller à remplir en temps voulu les conditions requises pour l'ouverture de la phase nationale. La majorité des offices désignés n'envoient pas de rappel à l'approche de la date limite pour aborder la phase nationale.

**Des informations détaillées concernant les actes de procédure à accomplir pour aborder la phase nationale auprès de chaque office désigné, les délais applicables et la possibilité d'obtenir une prolongation des délais ou un délai de grâce et toutes autres conditions applicables figurent dans le volume II du Guide du déposant du PCT. Les exigences concernant le dépôt d'une demande d'examen préliminaire international sont exposées dans le chapitre IX du volume I du Guide du déposant du PCT.**

GR et ES sont devenues liées par le chapitre II du PCT le 7 septembre 1996 et le 6 septembre 1997, respectivement, et peuvent donc être élues dans une demande d'examen préliminaire international ou dans une élection ultérieure présentée le 7 septembre 1996 (ou à une date postérieure) ou le 6 septembre 1997 (ou à une date postérieure), respectivement, quelle que soit la date de dépôt de la demande internationale (voir le second paragraphe, ci-dessus).

Veuillez noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

**CONFIRMATION DES DESIGNATIONS FAITES PAR MESURE DE PRECAUTION**

Seules les désignations expresses faites dans la requête conformément à la règle 4.9.a) figurent dans la présente notification. Il est important de vérifier si ces désignations ont été faites correctement. Des erreurs dans les désignations peuvent être corrigées lorsque des désignations ont été faites par mesure de précaution en vertu de la règle 4.9.b). Toute désignation ainsi faite peut être confirmée conformément aux dispositions de la règle 4.9.c) avant l'expiration d'un délai de 15 mois à compter de la date de priorité. En l'absence de confirmation, une désignation faite par mesure de précaution sera considérée comme retirée par le déposant. Il ne sera adressé aucun rappel ni invitation. Pour confirmer une désignation, il faut déposer une déclaration précisant l'Etat désigné concerné (avec l'indication de la forme de protection ou de traitement souhaitée) et payer les taxes de désignation et de confirmation. La confirmation doit parvenir à l'office récepteur dans le délai de 15 mois.

**EXIGENCES RELATIVES AUX DOCUMENTS DE PRIORITE**

Pour les déposants qui n'ont pas encore satisfait aux exigences relatives aux documents de priorité, il est rappelé ce qui suit.

Lorsque la priorité d'une demande nationale, régionale ou internationale antérieure est revendiquée, le déposant doit présenter une copie de cette demande antérieure, certifiée conforme par l'administration auprès de laquelle elle a été déposée ("document de priorité"), à l'office récepteur (qui la transmettra au Bureau international) ou directement au Bureau international, avant l'expiration d'un délai de 16 mois à compter de la date de priorité, étant entendu que tout document de priorité peut être présenté au Bureau international avant la date de publication de la demande internationale, auquel cas ce document sera réputé avoir été reçu par le Bureau international le dernier jour du délai de 16 mois (règle 17.1.a)).

Lorsque le document de priorité est délivré par l'office récepteur, le déposant peut, au lieu de présenter ce document, demander à l'office récepteur de le préparer et de le transmettre au Bureau international. La requête à cet effet doit être formulée avant l'expiration du délai de 16 mois et peut être soumise au paiement d'une taxe (règle 17.1.b)).

Si le document de priorité en question n'est pas fourni au Bureau international, ou si la demande adressée à l'office récepteur de préparer et de transmettre le document de priorité n'a pas été faite (et la taxe correspondante acquittée, le cas échéant) avant l'expiration du délai applicable mentionné aux paragraphes précédents, tout Etat désigné peut ne pas tenir compte de la revendication de priorité; toutefois, aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Lorsque plusieurs priorités sont revendiquées, la date de priorité à prendre en considération aux fins du calcul du délai de 16 mois est la date du dépôt de la demande la plus ancienne dont la priorité est revendiquée.

**THIS PAGE BLANK (USPTO)**

Suite du formulaire PCT/IB/308

**AVIS INFORMANT LE DEPOSANT DE LA COMMUNICATION DE  
LA DEMANDE INTERNATIONALE AUX OFFICES DESIGNES**

<b>Date d'expédition (jour/mois/année)</b> 03 mai 2001 (03.05.01)	<b>AVIS IMPORTANT</b>
<b>Référence du dossier du déposant ou du mandataire</b> PCT 3855/BC	<b>Demande internationale no</b> PCT/FR00/02979
<p>Il est notifié au déposant que, au moment de l'établissement du présent avis, le délai fixé à la règle 46.1 pour le dépôt de modifications selon l'article 19 n'était pas encore expiré et que le Bureau international n'avait pas reçu de modifications ni de déclaration l'informant que le déposant ne souhaitait pas présenter de modifications.</p>	

**THIS PAGE BLANK (USPTO)**



## TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

AVIS INFORMANT LE DEPOSANT DE LA  
COMMUNICATION DE LA DEMANDE  
INTERNATIONALE AUX OFFICES DESIGNES

(règle 47.1.c), première phrase, du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

CORLU, Bernard  
Bull S.A.  
PC58D20  
68, route de Versailles  
F-78434 Louveciennes Cedex  
FRANCE

Date d'expédition (jour/mois/année) 03 mai 2001 (03.05.01)		AVIS IMPORTANT	
Référence du dossier du déposant ou du mandataire PCT 3855/BC			
Demande internationale no PCT/FR00/02979	Date du dépôt international (jour/mois/année) 26 octobre 2000 (26.10.00)	Date de priorité (jour/mois/année) 28 octobre 1999 (28.10.99)	
Déposant BULL CP8 etc			

1. Il est notifié par la présente qu'à la date indiquée ci-dessus comme date d'expédition de cet avis, le Bureau international a communiqué, comme le prévoit l'article 20, la demande internationale aux offices désignés suivants:  
**AU,KR,US**

Conformément à la règle 47.1.c), troisième phrase, ces offices acceptent le présent avis comme preuve déterminante du fait que la communication de la demande internationale a bien eu lieu à la date d'expédition indiquée plus haut, et le déposant n'est pas tenu de remettre de copie de la demande internationale à l'office ou aux offices désignés.

2. Les offices désignés suivants ont renoncé à l'exigence selon laquelle cette communication doit être effectuée à cette date:  
**CN,EP,JP,SG**

La communication sera effectuée seulement sur demande de ces offices. De plus, le déposant n'est pas tenu de remettre de copie de la demande internationale aux offices en question (règle 49.1)a-bis)).

3. Le présent avis est accompagné d'une copie de la demande internationale publiée par le Bureau international le  
03 mai 2001 (03.05.01) sous le numéro WO 01/31880

**RAPPEL CONCERNANT LE CHAPITRE II (article 31.2)a) et règle 54.2)**

Si le déposant souhaite reporter l'ouverture de la phase nationale jusqu'à 30 mois (ou plus pour ce qui concerne certains offices) à compter de la date de priorité, la demande d'examen préliminaire international doit être présentée à l'administration compétente chargée de l'examen préliminaire international avant l'expiration d'un délai de 19 mois à compter de la date de priorité.

Il appartient exclusivement au déposant de veiller au respect du délai de 19 mois.

Il est à noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

**RAPPEL CONCERNANT L'OUVERTURE DE LA PHASE NATIONALE (article 22 ou 39.1))**

Si le déposant souhaite que la demande internationale procède en phase nationale, il doit, dans le délai de 20 mois ou de 30 mois, ou plus pour ce qui concerne certains offices, accomplir les actes mentionnés dans ces dispositions auprès de chaque office désigné ou élu.

Pour d'autres informations importantes concernant les délais et les actes à accomplir pour l'ouverture de la phase nationale, voir l'annexe du formulaire PCT/IB/301 (Notification de la réception de l'exemplaire original) et le volume II du Guide du déposant du PCT.

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse	Fonctionnaire autorisé J. Zahra
no de télécopieur (41-22) 740.14.35	no de téléphone (41-22) 338.83.38

**THIS PAGE BLANK (USPTO)**

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION  
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété  
Intellectuelle  
Bureau international



(43) Date de la publication internationale  
3 mai 2001 (03.05.2001)

PCT

(10) Numéro de publication internationale  
**WO 01/31880 A1**

(51) Classification internationale des brevets<sup>7</sup>: H04L 29/06

(21) Numéro de la demande internationale:

PCT/FR00/02979

(22) Date de dépôt international:

26 octobre 2000 (26.10.2000)

(25) Langue de dépôt:

français

(26) Langue de publication:

français

(30) Données relatives à la priorité:

99/13508

28 octobre 1999 (28.10.1999)

FR

(71) Déposant (pour tous les États désignés sauf US): **BULL CP8** [FR/FR]; 68, route de Versailles, B.P. 45, F-78430 Louveciennes (FR).

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement): **MARIANA, Renaud** [FR/FR]; 5, square Las Cases, F-78150 Le Chesnay (FR).

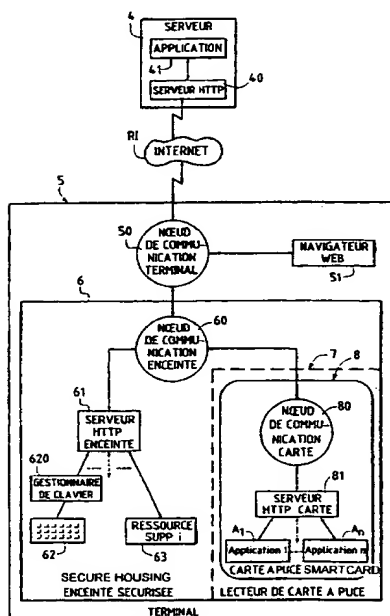
(74) Mandataire: **CORLU, Bernard**; Bull S.A., PC58D20, 68, route de Versailles, F-78434 Louveciennes Cedex (FR).

(81) États désignés (national): AU, CN, JP, KR, SG, US.

[Suite sur la page suivante]

(54) Title: SAFE TERMINAL PROVIDED WITH A SMART CARD READER DESIGNED TO COMMUNICATE WITH A SERVER VIA AN INTERNET-TYPE NETWORK

(54) Titre: TERMINAL SECURISE MUNI D'UN LECTEUR DE CARTE A PUCE DESTINE A COMMUNIQUER AVEC UN SERVEUR VIA UN RESEAU DE TYPE INTERNET



4...SERVER  
41...APPLICATION  
40...HTTP SERVER  
RI...INTERNET  
50...TERMINAL COMMUNICATION NODE  
51...WEB BROWSER  
60...HOUSING COMMUNICATION NODE  
61...HOUSING HTTP SERVER  
80...CARD COMMUNICATION NODE  
81...CARD HTTP SERVER  
7...SMART CARD READER  
63...SUPPLEMENTARY COMPUTER RESOURCES  
620...KEYBOARD MANAGER

(57) Abstract: The invention concerns a terminal architecture (5) for communications between a smart card (8) and a Web server (4), via an Internet-type network (RI). The terminal (5) is provided with a secure housing (6) comprising a smart card (8) reader, a keyboard (62), and, optionally, other computer resources (63). The non-secure part of the terminal (5) comprises a Web browser (51) and a first communication node (50) routing the received requests to the browser (51) or to the secure housing (6). The secure housing (6) comprises a second communication node (60) and a HTTP server (61). The smart card (8) comprises a third communication node (80) and a HTTP server (81). The Web server (4) comprises a transaction management and control application (41) capable of communicating with the smart card (8) and of activating the software applications (A<sub>1</sub> to A<sub>n</sub>) thereof.

(57) Abrégé: L'invention concerne une architecture de terminal (5) permettant des communications entre une carte à puce (8) et un serveur "WEB" (4), via un réseau de type Internet (RI). Le terminal (5) est muni d'une enceinte sécurisée (6) comprenant un lecteur de carte à puce (8), un clavier (62) et, de façon optionnelle, d'autres ressources informatiques (63). La partie non sécurisée du terminal (5) comprend un navigateur "WEB" (51) et un premier noeud communication (50) aiguillant les requêtes reçues vers le navigateur (51) ou vers l'enceinte sécurisée (6). L'enceinte sécurisée (6) comprend un deuxième noeud de communication (60) et un serveur "HTTP" (61). La carte à puce (8) comprend un troisième noeud de communication (80) et un serveur "HTTP" (81). Le serveur "WEB" (4) comprend une application marchande (41) pouvant être mise en communication avec la carte à puce (8) et activer des applications logicielles (A<sub>1</sub>-A<sub>n</sub>) de celle-ci.

WO 01/31880 A1



(84) États désignés (régional): brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

**Publiée:**

- Avec rapport de recherche internationale.
- Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.

## TERMINAL SECURISE MUNI D'UN LECTEUR DE CARTE A PUCE DESTINE A COMMUNIQUER AVEC UN SERVEUR VIA UN RESEAU DE TYPE INTERNET

L'invention concerne une architecture de terminal, plus particulièrement un terminal du type mettant en œuvre un clavier et un lecteur de carte à puce situés dans une enceinte sécurisée, et destiné à communiquer avec un serveur, via un réseau de type Internet.

5 Un tel dispositif est connu, par exemple, sous la dénomination commerciale "safepad".

Dans le cadre de l'invention, le terme "terminal" doit être compris dans un sens général. Le terminal précité peut être notamment constitué par un ordinateur personnel fonctionnant sous divers systèmes  
10 d'exploitation, tels WINDOWS ou UNIX (tous deux étant des marques déposées). Il peut être aussi constitué par une station de travail, un ordinateur portable ou un terminal de carte dit dédié.

De même, dans le cadre de l'invention, le terme "réseau Internet" englobe, outre le réseau Internet proprement dit, les réseaux privés  
15 d'entreprises ou similaires, dits "intranet", et les réseaux les prolongeant vers l'extérieur, dits "extranet".

Les cartes à puce sont utilisées dans divers domaines applications bancaires, de santé, comme "porte-monnaie" dit électronique, etc. Sur une carte à puce peuvent en outre coexister plusieurs applications  
20 (carte à puce multi-application).

Pour ces types d'applications, les carte à puce peuvent se voir dévolues diverses fonctions. En particulier, elles peuvent être utilisées à des fins de sécurité. Le terme "sécurité" doit être compris dans un sens général : notamment confidentialité et/ou authentification de l'utilisateur de  
25 la station et/ou du propriétaire de la carte à puce elle-même.

Dans ce cadre plus particulier d'applications, le terminal peut être muni d'une enceinte sécurisée comprenant un lecteur de carte à puce, un clavier et éventuellement une ou plusieurs autres ressources informatiques.

La figure 1 illustre très schématiquement l'architecture d'un terminal du type précité, selon l'art connu.

Pour fixer les idées, on va supposer que le terminal 1 est constitué à base d'un micro-ordinateur. Celui-ci est muni de tous les organes habituels constitutifs de tels appareils informatiques et nécessaires à leur bon fonctionnement (et qui n'ont pas été représentés) : unité centrale, mémoire vive, mémoire de masse (disque dur), lecteur(s) de support d'information (disquettes, etc.), etc. Dans le cas particulier illustré sur la figure 1, le terminal 1 est muni d'une enceinte sécurisée 3 comprenant un lecteur 30 de carte à puce 2 et un clavier 31. Le clavier 31 sert notamment à la saisie de données d'authentification du possesseur de la carte à puce 2 : par exemple un mot de passe associé à un identifiant de la carte à puce 2. Divers circuits électroniques permettent une communication entre les éléments sécurisés présents dans cette enceinte, notamment le clavier 31 et la carte à puce 2 (via le lecteur 30), d'une part, et ces éléments sécurisés et les éléments non sécurisés présents dans le terminal 1, d'autre part.

Habituellement, le terminal comprend, dans sa partie non sécurisée, une application spécifique 10, que l'on appellera ci-après "marchande", assurant la gestion et le contrôle de transactions particulières permises par le terminal 1 en question. Les communications entre cette application 10 et les éléments internes à l'enceinte sécurisée 3 s'effectuent habituellement selon un standard du type "RS232". Les communications entre les éléments internes à l'enceinte sécurisée 3, notamment une application résidente 300, et la carte à puce 2, via le lecteur 30, s'effectuent habituellement selon un protocole obéissant aux normes ISO 7816-1 à 7816-4.

Ce type d'architecture présente donc comme premiers inconvénients, notamment les suivants :

- l'application marchande implantée dans le terminal (partie non sécurisée) et celle résidente dans l'enceinte sécurisée sont spécifiques à ce terminal ;
- les programmes informatiques associés sont en général volumineux ; et

- la souplesse et la fiabilité sont limitées, car une modification de ces programmes nécessite un rechargement de programmes dans le terminal (partie non sécurisée) et dans l'enceinte sécurisée, ainsi qu'éventuellement l'exécution de tests de bon fonctionnement, ce qui

5 nécessite la présence de personnel spécialisé.

Généralement, cette dernière opération doit être répétée pour un grand nombre de terminaux.

Il doit en outre être conservé à l'esprit qu'il s'agit d'applications en tout ou partie sécurisées. On doit donc pouvoir garantir, pour la mise à jour

10 de programmes, un niveau de sécurité déterminé, propre à l'application spécifique.

Le plus souvent, le terminal 1 n'est pas isolé, en ce sens qu'il est relié, via un réseau de transmission *RI*, à un ou plusieurs systèmes éloignés, dont un seul 4 a été illustré sur la figure 1. La nature du réseau *RI*

15 peut être très diverse, selon les applications envisagées (application bancaire, de santé, etc.). Il peut s'agir notamment du réseau Internet ou d'un réseau de ce type (intranet ou extranet), compte tenu du développement rapide de ce dernier type de réseau et des applications qui y font appel. De façon habituelle, l'architecture globale est du type dit

20 "client-serveur", le "serveur" étant généralement le système éloigné 4 et le "client" étant le terminal 1. Mais dans certaines circonstances, les rôles peuvent être inversés ou alternés pendant le temps d'une transaction.

Dans une telle architecture, les programmes associés à l'application spécifique 10 et à l'application 300, en présence d'une

25 modification de leur version, pour quelle que raison que ce soit, peuvent alors être mis à jour de façon centralisée, à partir d'un des serveurs éloignés, par exemple le serveur 4. Il s'ensuit qu'un des inconvénients signalés peut être atténué, la mise à jour étant effectuée par télétraitement. Ces opérations nécessitent cependant la mise en œuvre de procédures

30 d'administration bien rodées. En outre, le téléchargement peut comprendre des données sensibles ou pour le moins ne doit pas autoriser l'implantation dans le terminal de programmes et/ou procédures non autorisés ou

dangereux pour la sécurité ("cheval de Troie", "bombes logiques", virus, etc.).

En outre, avec la montée en puissance et l'universalité du réseau Internet, le besoin se fait sentir de "faire migrer" les applications spécifiques précitées, implantées localement dans les terminaux, vers les serveurs éloignés, que l'on appellera ci après "serveurs marchands", d'une part, et de dialoguer directement avec la carte à puce, à partir de ces serveurs marchands, d'autre part.

Ce second besoin, en particulier, ne peut être satisfait par les terminaux de l'art connu, pour des raisons qui vont être explicitées ci-après.

Mais tout d'abord, il paraît utile de décrire brièvement une architecture de système permettant la communication entre un terminal selon l'art connu et un serveur éloigné, via un réseau de type Internet RI. Une telle architecture est représentée schématiquement sur la figure 2, figure sur laquelle a été représentée plus particulièrement l'architecture logique du terminal, référencé 1'.

Le terminal 1' est ici un terminal d'un type général, sécurisé ou non, cette disposition n'étant pas importante pour expliciter les différents types de communications en cause.

Comme il a été indiqué précédemment, le terminal 1' comprend naturellement tous les circuits et organes nécessaires à son bon fonctionnement, et qui n'ont pas été représentés dans un but de simplification du dessin. Habituellement, le terminal 1' est aussi relié à des périphériques classiques, intégrés ou non, tels un écran de visualisation (non représenté) et un clavier 31, situé dans une enceinte sécurisée (figure 1 : 3) dans le cadre plus particulier de l'invention.

Habituellement, les communications sur les réseaux s'effectuent conformément à des protocoles répondant à des standards comprenant plusieurs couches logicielles superposées. Dans le cas d'un réseau RI de type Internet, les communications s'effectuent selon des protocoles spécifiques à ce type de communication, mais qui comprennent aussi plusieurs couches logicielles. Le protocole de communication est choisi en



fonction de l'application plus particulièrement visée : interrogation de pages "WEB", transferts de fichiers, courrier électronique (e-mel, ou "e-mail" selon la terminologie anglo-saxonne), forums ou "news", etc.

5 L'architecture des réseaux de communication est décrite par diverses couches. A titre d'exemple, le standard "OSI" ("Open System Interconnection"), défini par l' "ISO", comporte sept couches qui vont des couches dites basses (par exemple la couche dite "physique" qui concerne le support de transmission physique) aux couches dites hautes (par exemple la couche dite "d'application"), en passant par des couches  
10 intermédiaires, notamment la couche dite de "transport". Une couche donnée offre ses services à la couche qui lui est immédiatement supérieure et requiert de la couche qui lui est immédiatement inférieure d'autres services, via des interfaces appropriées. Les couches communiquent à l'aide de primitives. Elles peuvent également communiquer avec des  
15 couches de même niveau. Dans certaines architectures, l'une ou l'autre de ces couches peut être inexistante.

Dans un environnement Internet, les couches sont au nombre de cinq, et de façon plus précise, en allant de la couche supérieure à la couche inférieure : la couche d'applications ("http", "ftp", "e-mail", etc.), la couche  
20 de transport ("TCP"), la couche d'adressage de réseau ("IP"), la couche de liens de données ("PPP", "Slip", etc.) et la couche physique.

Le terminal 1' comprend des circuits d'accès 11 au réseau Internet. Il peut s'agir d'un modem pour se connecter à une ligne téléphonique commutée ou à un réseau numérique à intégration de services ("RNIS"), via  
25 par exemple un prestataire de services Internet ("Internet Service Provider" ou "ISP", selon la terminologie anglo-saxonne). Les circuits 11 d'accès au réseau *R/* regroupent les couches logicielles inférieures C1 et C2, correspondant aux couches "physique" et de "lien de données" précitées.

On a également représenté les couches supérieures C3 et C4,  
30 correspondant aux couches "d'adressage de réseau" ("IP") et de "transport" ("TCP"). La couche supérieure d'application ("http", "ftp", "e-mail", etc.) est

schématisée par un navigateur "WEB" NW de type quelconque, de préférence d'un type standard du commerce.

L'interface entre les couches inférieures, C<sub>1</sub> et C<sub>2</sub>, et les couches supérieures, C<sub>3</sub> et C<sub>4</sub>, est constituée par une couche logicielle 15 généralement appelée "driver couches basses". Les couches supérieures, C<sub>3</sub> et C<sub>4</sub>, s'appuient sur cette interface et sont mises en œuvre par l'intermédiaire de bibliothèques de fonctions spécifiques ou bibliothèques réseau 14, avec lesquelles elles correspondent. Dans le cas du réseau Internet, "TCP/IP" est mis en œuvre au moyen de bibliothèques dites de "sockets".

Cette organisation permet au navigateur NW de poser des requêtes vers un serveur éloigné 4, pour la consultation de pages ""WEB"" (protocole "HTTP"), pour le transfert de fichiers (protocole "FTP") ou l'envoi de courrier électronique (protocole "e-mail").

Le terminal 1' comprend également le lecteur de carte 30 situé dans une enceinte sécurisée (figure 1 : 3), dans le cadre plus particulier de l'invention. Pour communiquer avec la carte à puce 2, le lecteur de carte 30 englobe également deux couches basses, CC<sub>1</sub> (couche physique) et CC<sub>2</sub> (couche de lien de données), jouant un rôle similaire aux couches C<sub>1</sub> et C<sub>2</sub>. Les interfaces logicielles avec les couches CC<sub>1</sub> et CC<sub>2</sub> sont décrites, par exemple, par la spécification "PC/SC" ("part 6, service provider"). Les couches elles-mêmes, CC<sub>1</sub> et CC<sub>2</sub>, sont notamment décrites par les normes ISO 7816-1 à 7816-4.

Une couche logicielle supplémentaire 13 forme interface entre des couches applicatives, sous la référence unique *Appli*<sub>i</sub>, et les couches inférieures, CC<sub>1</sub> et CC<sub>2</sub>. La fonction principale dévolue à cette couche 13 est une fonction de multiplexage/démultiplexage.

Du côté de la carte à puce 2, on retrouve une organisation similaire, à savoir la présence de deux couches basses, référencées CC'<sub>1</sub> (couche physique) et CC'<sub>2</sub> (couche de lien de données), ainsi qu'une couche d'interface 23, tout à fait similaire à la couche 13. Cette couche 23

assure une interface entre les couches protocolaires CC'1 et CC'2 précitées et une ou plusieurs couches applicatives, représentées sous la forme d'un module unique référencée *Appli<sub>2</sub>*.

5 Les communications entre le lecteur de carte à puce 30 et la carte à puce 2 s'effectuent à l'aide de commandes standardisées, connues sous l'abréviation anglo-saxonne de "APDU" (pour "Application Protocol Data Unit").

Différents protocoles sont utilisables, et à titre d'exemples non exhaustifs les suivants :

- 10
- la recommandation ETSI GSM 11.11 ;
  - le protocole défini par la norme ISO 7816-3, en mode caractère T=0 ;
  - le protocole défini par la norme ISO 7816-3, en mode bloc T=1 ;
  - ou le protocole défini par la norme ISO 3309, en mode trame "HDLC" (pour "High-Level Data Link Control procedure" ou procédure de
- 15 commande de liaison à haut niveau).

Dans le cadre de l'invention, on utilisera de préférence le protocole ISO 7816-3, en mode bloc.

De façon connue en soi, à chaque couche de protocole, il est associé un certain nombre de primitives qui permettent les échanges de données entre couches de même niveau et d'une couche à l'autre.

20

Dans l'état actuel de la technique, il n'est pas possible de mettre en communication directe la carte à puce 2 avec un serveur éloigné 4, via le réseau Internet *RI*, car le protocole de communication entre une carte à puce 2 d'un type standard, qui vient d'être rappelé, est incompatible avec ceux utilisés sur le réseau Internet ou tout réseau de ce type. Il n'est pas

25 non plus possible d'établir des communications directes entre le navigateur *NW* et la carte à puce 2, sauf à implanter dans le navigateur *NW* une pièce de logiciel, dit "plug-in", d'un type spécifique.

Si on se reporte de nouveau à la figure 1, en supposant que le terminal 1 est relié au réseau Internet, et en résumé de ce qui vient d'être

30 rappelé, on constate que ce terminal 1, selon l'art connu, comprenant une enceinte sécurisée 3 munie d'un clavier 31 et d'un lecteur 30 de carte à

puce 2, comporte deux interfaces principales de communication,  $S_1$  et  $S_2$ , représentées en traits pointillés. Une première interface,  $S_1$ , relie l'enceinte 3 au terminal 1 proprement dit, où s'exécute l'application marchande 10, et une deuxième interface,  $S_2$ , est prévue pour les communications avec la

5 carte à puce 2. En réalité, l'interface  $S_2$  est répartie entre l'application 300 et la carte à puce 2. A ces deux interfaces s'ajoute en outre l'interface vers l'extérieur (figure 2 : circuits 11 notamment), qui permet au terminal 1 de communiquer avec le réseau Internet  $R/I$ . L'interface  $S_1$  accepte deux

10 niveaux de dialogue : un premier dialogue transparent pour lequel un ordre émis par le terminal 1 s'exécute sans modification sémantique par l'interface  $S_2$ , et un second niveau de dialogue qui fait intervenir l'application 300.

Ainsi l'authentification par saisie de mot de passe sur le clavier 31 est un ordre soumis à l'interface  $S_1$  qui est interprété par l'application 300 et transformé en une succession d'échanges sur l'interface  $S_2$ , entre

15 l'application 300 et la carte à puce 2. Le résultat de ces échanges est transmis à l'interface  $S_1$ .

Outre le fait, qu'il est exclu, dans l'état actuel de la technique, qu'une carte à puce standard 2 accepte des échanges directs avec le réseau Internet  $R/I$ , comme il vient d'être rappelé, l'inconvénient majeur des

20 terminaux selon l'art connu est constitué par la présence de l'application résidente 300. Il s'agit le plus souvent d'une application dite "propriétaire", ce qui implique que l'application marchande 10 doit être écrite en fonction de la nature et du type de terminal utilisé. Elle est donc *a priori* différente d'un type de terminal à un autre, ce qui ne facilite pas les opérations de

25 maintenance. En outre, elle n'est pas non plus adaptée à un environnement de type Internet.

Il a été proposé des standards pour des applications du type de celle de l'invention, comme le standard connu sous le sigle anglo-saxon "OCF" (pour "Open Card Framework") qui tend à la standardisation des

30 échanges entre le terminal marchand 1 et le lecteur 30 de carte à puce 2, en respectant par exemple la norme "EMV" des terminaux. Cependant un tel standard n'est pas directement utilisable dans un contexte Internet.

Est également connu, dans le domaine des applications bancaires, le protocole dit "C-SET", protocole défini par le G.I.E. carte bancaire. Selon ce protocole, un utilisateur se connecte sur un site marchand disponible sur le "WEB" et procède à un achat. Ce dernier, lors de la transaction, sollicite des éléments de l'enceinte sécurisée pour authentifier le porteur de la carte bancaire effectuant l'achat. Cette authentification est effectuée par l'exécution d'un logiciel dans le terminal (partie non sécurisée) et l'enceinte.

Ce protocole n'est pas non plus exempt d'inconvénients :

- il rend nécessaire la présence d'un logiciel spécifique dans le terminal et dans l'enceinte ;

- il rend nécessaire la certification des logiciels imposés par "C-SET" ;

- le protocole "C-SET" est uniquement orienté paiement : le logiciel dans le terminal qui traite les informations du serveur "WEB" et du paiement par la carte bancaire est un logiciel de paiement.

Par ces caractéristiques, il ne diffère guère des solutions de l'art connu précédemment évoquées. Il ne permet pas des communications de bout en bout, selon un protocole de type Internet, notamment un adressage direct de la carte à puce. De par sa spécificité, il n'offre aucune flexibilité et n'est pas adapté pour une utilisation dans d'autres domaines : santé, mise à jour de données stockées sur une carte à puce, crédit de points, etc.

Tout en palliant les inconvénients des procédés et architectures de l'art connu, et dont certains viennent d'être rappelés, l'invention se fixe pour but de remplir les besoins qui se font sentir.

Elle favorise l'utilisation sur le réseau Internet de terminaux comprenant une enceinte sécurisée munie d'au moins un lecteur de carte à puce et d'un clavier, en permettant la migration des applications des lecteurs de carte à puce et des terminaux vers un serveur éloigné de type "WEB", d'une part, et le dialogue direct avec la carte à puce, d'autre part.

Elle permet une mise à jour ou un ajout de logiciel interne à l'enceinte sécurisée, avec un maximum de sécurité.

Pour ce faire, selon un premier aspect de l'invention, la carte à puce n'est plus adressée de façon classique par des "APDU", conformément au protocole de communication ISO 7816 précité, mais par utilisation d'une adresse "URL" (pour "Universal Resource Location").

5 Comme il est connu, une adresse "URL" est constituée d'une adresse "IP" proprement dite et d'un numéro de port. De la même manière, l'enceinte sécurisée utilise cet adressage par "URL".

Selon un aspect de l'invention, la carte à puce se comporte donc aussi comme un serveur et/ou client "WEB".

10 L'enceinte sécurisée selon l'invention est "transparente" pour le réseau Internet, en ce sens que les "ordres carte" émanant du serveur marchand éloigné ne font pas intervenir d'éléments d'adressage du terminal. Il s'ensuit que les ressources associées à l'enceinte sécurisée ne sont pas accessibles du réseau Internet. Par contre, les applications

15 contenues dans la carte à puce ont la possibilité d'adresser et d'activer toutes les ressources informatiques présentes dans l'enceinte sécurisée, notamment un clavier, par simple adressage "URL" comme il sera explicité ci-après.

Pour ce faire, le terminal comprend physiquement :

- 20 - une enceinte sécurisée d'un type modifié, comprenant au moins un lecteur de carte à puce et un clavier (et/ou une autre ressource informatique), tous deux rattachés à un serveur "HTTP" dit d'enceinte sécurisée, ainsi qu'une unité d'exécution qui gère l'ensemble des ressources présentes dans l'enceinte ; et
- 25 - outre des éléments classiques (mémoires, etc.) et un navigateur de type "WEB", un premier nœud de communication, dit de terminal, assurant des communications entre le réseau Internet, le navigateur de type "WEB" et/ou l'enceinte sécurisée.

30 Par ailleurs, l'enceinte sécurisée précitée comprend un deuxième nœud de communication, dit d'enceinte, assurant des communications entre le terminal proprement dit, via le premier nœud de communication, le serveur "HTTP" dit d'enceinte sécurisée, et/ou le lecteur de carte à puce.

La carte à puce est elle-même munie d'un troisième nœud de communication, dit de carte, et d'une adaptation logicielle se comportant comme un serveur "HTTP", formant interface entre au moins une application résidente dans la carte à puce et le deuxième nœud de communication.

5 Le premier nœud de communication aiguille les requêtes du réseau Internet ayant un numéro de port associé à l'enceinte sécurisée vers cette enceinte et effectue les adaptations de protocoles nécessaires pour mettre en communication directe le réseau Internet avec le deuxième nœud de communication, et assurer une propagation d'informations et/ou d'ordres  
10 vers la carte à puce.

Pour certaines applications, notamment des applications exigeant un haut niveau de sécurité, l'enceinte sécurisée peut comprendre avantageusement une ou plusieurs ressource(s) informatique(s) supplémentaire(s), tels par exemple des dispositifs d'authentification  
15 biométriques (reconnaissance oculaire, vocale et/ou de signature), un coprocesseur ou un interpréteur externe.

Dans une variante préférée du procédé selon l'invention, les programmes nécessaires au fonctionnement des éléments et ressources de l'enceinte sécurisée, ou leurs mises à jour, sont téléchargés, via le réseau  
20 Internet, depuis un serveur "WEB" distant relié à ce réseau. La mise à jour peut inclure l'effacement, au moins partiel de ces programmes.

On prévoit également, dans des variantes de réalisation supplémentaires, de télécharger, mettre à jour et/ou supprimer des applications ou parties d'applications enregistrées dans la carte à puce  
25 (fichiers, programmes, scripts, etc.), via le réseau Internet et les nœuds de communication.

Toutes ces opérations peuvent s'effectuer dans de très bonnes conditions de sécurité, du fait de la transparence précitée de l'enceinte sécurisée vis-à-vis du réseau Internet.

30 L'invention a donc pour objet principal un terminal muni d'une enceinte sécurisée destinée à communiquer avec au moins un serveur de type "WEB", via un réseau de type Internet, selon un premier protocole de

communication de type Internet, ladite enceinte sécurisée comprenant au moins un lecteur de carte à puce, ladite carte à puce stockant au moins une application logicielle, caractérisé en ce que ledit terminal comprend une

5 partie non sécurisée comprenant au moins un premier module dit premier nœud de communication, ladite enceinte sécurisée comprend au moins un deuxième module dit deuxième nœud de communication et ladite carte à puce comprend au moins un troisième module dit troisième nœud de communication, en ce que lesdits nœuds de communication comprennent

10 des première, deuxième et troisième piles protocolaires, respectivement, comprenant chacune un nombre déterminé de couches logicielles de communication dites standards et des première, deuxième et troisième pièces de logiciel spécifique, respectivement, comprenant chacune au moins une première entité logicielle, lesdites premières entités logicielles étant appariées deux à deux, en ce que ledit premier nœud autorise au

15 moins des communications entre ledit terminal et ledit serveur "WEB", selon ledit premier protocole de communication de type Internet, en ce que lesdites premières entités desdites première et deuxième pièces de logiciel spécifique autorisent l'établissement d'une session d'échanges de données bilatéraux entre ledit terminal et la dite enceinte sécurisée, selon un

20 deuxième protocole de communication déterminé, en ce que lesdites premières entités desdites deuxième et troisième pièces de logiciel spécifique autorisent au moins l'établissement d'une session d'échanges de données bilatéraux entre la dite enceinte sécurisée et ladite carte à puce, via ledit lecteur de carte à puce, selon un troisième protocole de

25 communication déterminé, de manière à pouvoir mettre en relation au moins une desdites applications logicielles de la carte à puce avec ledit serveur de type "WEB".

L'invention va maintenant être décrite de façon plus détaillée en se référant aux dessins annexés, parmi lesquels :

- 30 - la figure 1 illustre schématiquement un exemple de terminal selon l'art connu comprenant une enceinte sécurisée munie d'un lecteur de carte à puce et un clavier ;



## 13

- la figure 2 illustre de façon générale l'architecture logique d'un terminal selon l'art connu comprenant un lecteur de carte à puce et communiquant avec un serveur "WEB" via le réseau Internet ;
- la figure 3 illustre schématiquement un exemple d'architecture générale selon l'invention permettant des communications, via le réseau Internet, entre un serveur éloigné, dit marchand, et un terminal muni d'une enceinte sécurisée comprenant un lecteur de carte à puce, un clavier et d'autres ressources informatiques ;
- la figure 4 illustre l'architecture logique de modules permettant les communications entre l'enceinte sécurisée du terminal de la figure 3 et la carte à puce ; et
- la figure 5 illustre un mode de réalisation particulier de l'architecture logique de la carte à puce.

On va maintenant décrire un exemple de réalisation de terminal à enceinte sécurisée conforme à l'invention et l'architecture de système de communication entre ce terminal et un serveur dit "marchand", par référence à la figure 3.

Le terminal, désormais référencé 5, peut être réalisé, comme il a été indiqué, à base d'un micro-ordinateur ou d'un appareil similaire. Il comprend un certain nombre d'éléments classiques : microprocesseur, mémoires vive et morte, mémoire de masse (disque dur, etc.), etc. qui ne sont pas représentés et sont bien connus de l'Homme de Métier. Par contre, dans l'application propre à l'invention, le terminal 5 comprend une enceinte 6, sécurisée par des moyens physiques et logiques, connus en soi. Cette enceinte sécurisée 6 comprend des éléments communs à l'art connu, mais aussi des éléments spécifiques à l'invention et qui seront précisés ci-après. Elle comprend tout d'abord, comme dans l'art connu, un clavier 62, son gestionnaire 620, ou "handler" selon la terminologie anglo-saxonne, et un lecteur de carte à puce 7.

Le terminal 5 est connecté à un serveur éloigné 4 via le réseau Internet RI ou tout réseau de ce type (intranet, extranet). Comme dans le cas de la figure 2, il comprend donc tous les éléments logiques et matériels

permettant de communiquer selon un des protocoles utilisés sur le réseau Internet, notamment le protocole "HTTP/TCP-IP". Il est donc inutile de redécrire ces éléments, sauf à mentionner qu'il comprend un navigateur de type "WEB" référencé 51. Ce navigateur 51 permet notamment de poser  
5 des requêtes vers le serveur 4. Il constitue une des applications présentes dans le terminal 5, celui-ci pouvant en effet en comporter une pluralité.

Selon une première caractéristique de l'invention, les applications spécifiques de l'application marchande ont migré vers le serveur 4. Ce dernier comprend donc notamment un serveur "HTTP" proprement dit 40 et  
10 les applications marchandes précitées, enregistrées dans des moyens de mémoires 41.

Selon une autre caractéristique de l'invention, le terminal comprend un premier module spécifique 50, que l'on appellera premier nœud de communication ou "nœud de communication terminal". Ce module 50  
15 comprend des moyens classiques de communication, notamment les piles protocolaires décrites en relation avec la figure 2, mais aussi des éléments spécifiques qui seront décrits ultérieurement.

Selon une autre caractéristique encore, l'enceinte sécurisée 6 comprend aussi un module spécifique 60, que l'on appellera deuxième  
20 nœud de communication ou "nœud de communication enceinte".

Le premier nœud de communication, 50, permet de faire communiquer les serveurs du réseau *R/I*, par exemple le serveur 4, ainsi que les applications présentes dans la partie non sécurisée du terminal 5 (par exemple le navigateur "WEB" 51) avec les éléments présents dans  
25 l'enceinte sécurisée 6, notamment le lecteur de carte à puce 7 et la carte à puce 8, via le deuxième nœud de communication 60.

L'enceinte sécurisée 6 comprend un serveur "HTTP" 61, que l'on appellera serveur "HTTP enceinte", disposé entre le deuxième nœud de communication 60 et le clavier 62. Ce dernier constitue l'une des  
30 ressources informatiques de l'enceinte sécurisée 6. Cette dernière, comme il a été indiqué dans le préambule de la présente description, peut comprendre des ressources supplémentaires 1 à *i*, représentées sous la

## 15

référence unique 63. Il peut s'agir, par exemple, de dispositifs d'authentification biométriques, d'un coprocesseur ou d'un interpréteur externe. La ou les ressource(s) 63 est (sont) également connectée(s) au serveur "HTTP" 61, de manière similaire au clavier 62.

5 Le serveur "HTTP" 61 est également connecté au lecteur de carte à puce 7.

Le nœud de communication 60 permet d'aiguiller les requêtes du terminal 5 vers la carte à puce 8, via le lecteur de carte à puce 7, de diriger, en sens inverse, les requêtes de la carte à puce 8, soit vers le serveur "HTTP" 61, soit vers le terminal 5, via le nœud de communication 50.

Selon un aspect de l'invention, le serveur "HTTP" 61 permet à la carte à puce 8, et uniquement à celle-ci, d'utiliser les ressources, 62 à 63, de l'enceinte sécurisée 6.

15 L'impossibilité d'accéder aux informations du clavier 62 ou des autres ressources 63, autrement qu'en passant par la carte à puce 8, qui joue un rôle d'intermédiaire, est due à plusieurs facteurs :

a/ l'enceinte 6 est physiquement sécurisée (impossibilité physique "d'espionner" les éléments) ;

20 b/ la programmation du nœud 60 est telle que celui-ci empêche tout routage de données provenant de l'extérieur vers l'entité "HTTP enceinte" 61, le nœud 60 étant par ailleurs protégé, puisque situé à l'intérieur de l'enceinte sécurisée 6 ; et

25 c/ la programmation de l'entité "HTTP enceinte" 61 est telle que cette dernière n'accepte pas de requêtes autres que celles émanant de la carte à puce 8, ce serveur 61 étant aussi protégé, puisque également situé à l'intérieur de l'enceinte sécurisée 6.

Si le point a/ est, en soi, commun à l'art connu et à l'invention, les points b/ et c/ constituent des caractéristiques spécifiques et avantageuses de l'invention.

30 On va maintenant décrire de façon plus détaillée comment s'effectuent les communications entre le réseau Internet *R*/ et les éléments de la partie non sécurisée du terminal 5, entre ces derniers et ceux de

## 16

l'enceinte sécurisée 6, entre les éléments de l'enceinte sécurisée 6, et entre ces derniers et la carte à puce 8, via le lecteur de carte à puce 7.

5 Selon l'une des caractéristiques principales de l'invention, toutes ces communications s'effectuent selon un mode que l'on qualifiera "d'homogène", tout à la fois compatible avec les protocoles Internet, par utilisation d'adresse de type standard "URL", et conservant les protocoles normalisés de communication, notamment entre la carte à puce 8 et le lecteur de carte à puce 7 (c'est-à-dire conformes aux normes ISO 7816 précitées).

10 Les communications entre le navigateur "WEB" 51 et le serveur "marchand" 4 ne posent pas de problèmes particuliers et peuvent s'effectuer normalement selon le protocole "HTTP", par utilisation de couches protocolaires classiques (voir figure 2) et d'un adressage "URL". Par contre, comme il a été rappelé, dans l'art connu, il n'en est pas de même entre les éléments non sécurisés et sécurisés d'un terminal (figure 1 : 15 1) où les communications sont habituellement effectuées en mode RS232, ni entre les éléments de l'enceinte sécurisée 6 et la carte à puce 8, via le lecteur 7. Dans ce dernier cas, comme il a été explicité en regard de la figure 2, les communications s'effectuent, certes par mise en œuvre de couches protocolaires, mais à l'aide d'un jeu d'ordres "APDU", 20 conformément à la norme ISO 7816-3 précitée, donc aussi de façon incompatible avec un protocole de type Internet.

Aussi, l'invention propose des dispositions spécifiques permettant d'unifier les communications, tout en conservant la standardisation des éléments entrant en jeu dans les communications et en ne conduisant qu'à 25 des modifications mineures.

On va tout d'abord détailler les modifications à apporter à l'enceinte sécurisée 6 et à la carte à puce 8, pour pouvoir assurer des communications entre ces deux entités, de façon conforme à l'invention.

30 Selon une caractéristique de l'invention, on munit la carte à puce 8 d'un module spécifique constituant un troisième nœud de communication 80 et un serveur "HTTP" 81, que l'on appellera ci-après respectivement "nœud

de communication carte" et "serveur HTTP de carte". La ou les  $n$  application(s) présente(s) dans la carte à puce 8,  $A_1$  à  $A_n$ , sont connectées par une première face du serveur "HTTP" 81. Par ces dispositions, la carte à puce 8 est transformée en serveur et/ou client "WEB" pour l'enceinte sécurisée 6 et peut être "adressée" par une adresse "URL".

Cette architecture est obtenue, selon l'invention, essentiellement en implantant une première couche de protocole de communication spécifique dans la carte à puce 8. De même, une deuxième couche de protocole de communication spécifique, formant le pendant de la première, est implantée dans l'enceinte sécurisée 6.

En ce qui concerne les échanges entre carte à puce 8 et enceinte sécurisée 6, le schéma fonctionnel de la figure 3 peut être représenté par l'architecture logique illustrée par la figure 4.

Dans cette architecture, on retrouve les couches protocolaires de l'art connu, comme illustré par la figure 2, qui jouent les mêmes rôles et portent les mêmes références. Il est donc inutile de les re-décrire.

Par contre, on prévoit, de part et d'autre, c'est-à-dire dans l'enceinte sécurisée 6 et dans la carte à puce 8, deux couches de protocoles spécifiques supplémentaires : 64 et 84, respectivement.

Dans l'enceinte sécurisée 6, la couche spécifique 64 s'interface aux couches protocolaires du lecteur de carte 3, c'est-à-dire les couches inférieures, CC1 et CC2, via la couche de multiplexage 13. La couche spécifique 64 permet le transfert de paquets de données de et vers la carte à puce 8. En outre, elle adapte les applications existantes pour des utilisations mettant en œuvre la carte à puce 8, sans devoir les réécrire.

Du côté de la carte à puce 8, on retrouve une organisation tout à fait similaire constituée par une instance supplémentaire de la couche spécifique, référencée 84, pendant de la couche 64.

De façon plus précise, les couches spécifiques, 64 et 84, sont subdivisées en trois éléments logiciels principaux :

- un module, 640 ou 840, de transfert de blocs d'informations entre les couches 13 et 23, via les couches conventionnelles CC<sub>1</sub>, CC<sub>2</sub>, CC'<sub>1</sub> et CC'<sub>2</sub> ;

- une ou plusieurs pièces de logiciel, dites "agents intelligents", 641 ou 841, qui réalisent, par exemple, des fonctions de conversion de protocoles ;

- et un module de gestion de la configuration spécifique, 642 et 842, respectivement, module qui peut être assimilé à un agent intelligent particulier.

10 On retrouve donc, dans l'enceinte sécurisée 6 et la carte à puce 8, une pile protocolaire de communication entre les deux entités.

Les couches de niveau deux (couches de lien de données), CC<sub>2</sub> et CC'<sub>2</sub>, assurent les échanges entre la carte à puce 8 et l'enceinte sécurisée 6. Ces couches sont responsables de la détection et l'éventuelle  
15 correction d'erreurs de transmission. Les différents protocoles rappelés sont utilisables à cette fin (recommandation ETSI GSM 11.11 ; le protocole défini par la norme ISO 7816-3, en mode caractère T=0 ou en mode bloc T=1 ; ou le protocole défini par la norme ISO 3309, en mode trame "HDLC"). Il a été  
indiqué que, dans le cadre de l'invention, on utilise de préférence le  
20 protocole ISO 7816-3, en mode bloc.

De façon connue en soi, à chaque couche de protocole il est associé un certain nombre de primitives qui permettent les échanges de données entre couches de même niveau et d'une couche à l'autre. A titre d'exemple, les primitives associées à la couche de niveau deux sont du type  
25 "demande de données" ("*Data.request*") et "envoi de données" par la carte ("*Data.response*"), ainsi que "confirmation de données" ("*Data.confirm*"), etc.

De façon plus particulière, les couches spécifiques 64 et 84 sont chargées du dialogue entre la carte à puce 8 et l'hôte, c'est-à-dire l'enceinte  
30 sécurisée 6. Elles permettent aussi la mise en place d'une configuration adaptée pour l'émission et/ou la réception de paquets de données.

Comme il a été indiqué ci-dessus, les couches comprennent trois entités distinctes.

La première entité, les modules 640 ou 840, est essentiellement constituée par un multiplexeur logiciel. Elle permet l'échange d'informations  
5 entre la carte à puce 8 et le terminal hôte 6, sous la forme d'unités de données de protocole. Elle joue un rôle similaire à celui d'un commutateur de paquets de données. Ces unités sont émises ou reçues via la couche de niveau 2 (couche de liens de données). Ce protocole particulier de communication permet de mettre en communication au moins une paire d'  
10 "agents intelligents". Le premier agent de chaque paire, 641, est situé dans la couche 64, côté enceinte sécurisée 6, le second, 841, est situé dans la couche 84, côté carte à puce 8. Une liaison entre deux "agents intelligents" est associée à une session. Une session est un échange de données bidirectionnel entre ces deux agents.

15 Un agent intelligent peut réaliser tout ou partie des fonctions des couches de niveau trois et quatre, en fonction de la configuration mise en œuvre par l'enceinte sécurisée 6.

Un agent intelligent particulier est identifié avantageusement par un nombre entier, par exemple sur 16 bits (nombre compris entre 0 et 6535).  
20 Cet identificateur est utilisé, par exemple, dans une unité de donnée de protocole constituant une référence de destination et une référence de source.

Il existe deux grandes catégories d'agents intelligents : les agents de type "serveur", qui sont identifiés par une référence fixe, et les agents de  
25 type "client", qui sont identifiés par une référence variable, délivrée par le module de gestion de configuration, 642 ou 842.

Le processus d'ouverture d'une session est habituellement le suivant : un agent intelligent de type "client" ouvre la session vers un agent intelligent de type "serveur". Les modules 642 et 842 gèrent des tables (non  
30 représentées) qui contiennent la liste des agents intelligents présents, côté hôte 6 et carte à puce 8.

Les agents intelligents, 641 ou 841, sont associés à des propriétés ou attributs particuliers. Pour fixer les idées, et à titre d'exemple non limitatif, les quatre propriétés suivantes sont associées aux agents intelligents :

- 5           - "hôte" : agent localisé dans l'enceinte sécurisée ;
- "carte" : agent localisé dans la carte à puce ;
- "client" : agent qui initialise une session ;
- "serveur" : agent qui reçoit une demande de session.

Les agents intelligents permettent d'échanger des données.

- 10           Les modules de gestion de configuration, 642 et 842, respectivement, sont assimilables, comme il a été indiqué, à des agents intelligents particuliers. Par exemple, le module 642, côté hôte 6, gère notamment des informations relatives à la configuration de l'enceinte sécurisée 6 (modes de fonctionnement), liste des autres agents présents,
- 15           etc. Le module 842, côté carte à puce 8, a des fonctions analogues. Ces deux agents peuvent être mis en communication l'un avec l'autre pour établir une session.

- Selon une caractéristique de l'invention, la carte à puce 8 propose au système hôte, c'est-à-dire à l'enceinte 6, un modèle de terminal virtuel.
- 20           Pour ce faire, la carte à puce 8 se comporte comme un serveur et/ou client "WEB".

- De façon pratique, la carte à puce 8 est avantageusement "adressée" par utilisation d'une adresse "URL" définissant un rebouclage sur le terminal 5, et plus particulièrement sur l'enceinte sécurisée 6, et non
- 25           un pointage sur un serveur externe, tel le serveur 4. A titre d'exemple, la structure de cet "URL" est habituellement la suivante :

http://127.0.0.1:8080   (1) ou

http://localhost:8080   (1bis)

- dans laquelle 127.0.0.1 est l'adresse "IP" de rebouclage ("localhost" étant
- 30           la traduction littérale de 127.0.0.1) et 8080 est le numéro de port. L'adresse "URL" des ressources 62 et/ou 63 pourrait être complétée par un suffixe du



type "/xxx". Par exemple, le module de gestion 620 du clavier 62 pourrait avoir comme adresse "URL" la suivante :

http://localhost:8080/kb (2)

5 L'architecture logique permettant des communications entre le terminal 5 proprement dit (entre les nœuds 50 et 60), c'est-à-dire les éléments non sécurisés de celui-ci et l'enceinte sécurisée 6 est similaire à celle représentée sur la figure 4. En conséquence, des sessions vont pouvoir être établies entre les nœuds de communication 50 et 60 conformément au schéma général qui vient d'être décrit. L'enceinte  
10 sécurisée va notamment pouvoir être adressée par une adresse "URL", sous le même numéro de port que la carte à puce, soit 8080 dans l'exemple décrit.

Le nœud de communication 50 permet aussi au terminal 5 de communiquer avec le réseau Internet *RI*. Aussi, outre les propriétés  
15 associées aux agents intelligents qui ont été énumérées ci-dessus, il existe également les deux propriétés suivantes :

- "local" : agent ne communiquant pas avec le réseau ;
- "réseau" : agent communiquant avec le réseau ;

Le terminal 5, en sa globalité, est adressé par la même adresse  
20 "IP" que ci-dessus. Il héberge au moins une application dite de terminal, avantageusement le navigateur "WEB" 51. Celui-ci est associé à un port particulier.

A titre d'exemple, par une technique de page "WEB" et d'hyperliens, un utilisateur (non représenté) peut choisir un produit ou un  
25 service parmi ceux disponibles et transmettre la requête au serveur marchand 4.

Outre la fonction serveur-client "WEB" offerte par la carte à puce 8, selon un autre aspect de l'invention, il est inclus dans celle-ci un mécanisme similaire à la fonction dite "CGI" (pour "Common Gateway  
30 Interface") implantée dans les serveurs "WEB" classiques.

Avant de décrire un exemple d'une architecture conforme à l'invention, permettant de réaliser une fonction de ce type au sein même de

la carte à puce 8, il est utile de rappeler les principales caractéristiques d'un mode de fonctionnement "CGI".

5 Le "CGI" est une spécification de mise en œuvre, depuis un serveur "WEB", d'applications écrites pour les systèmes d'exploitation "UNIX" (marque déposée), "DOS", ou "WINDOWS" (marque déposée). A titre d'exemple, pour le système d'exploitation "UNIX", la spécification est "CGI 1.1" et pour le système d'exploitation "WINDOWS 95", la spécification est "CGI 1.3".

10 Toujours à titre d'exemple, une requête "HTTP" pour une adresse "URL", du type :

"http://www.host.com/cgi-bin/xxx" (3),

dans laquelle "host" se réfère à un système hôte (généralement éloigné), est interprétée par un serveur "WEB" comme l'exécution d'un script de commande, de type "CGI" nommé "xxx" et présent dans le répertoire "cgi-bin" de ce système hôte. Bien que le nom du répertoire puisse être *a priori* 15 quelconque, par convention, c'est le nom donné au répertoire stockant les scripts de type "CGI". Un script est une suite d'instructions du système d'exploitation du système hôte dont le résultat final est transmis au navigateur "WEB" émetteur de la requête précitée ou à toute autre 20 application sollicitant le service, comme un serveur marchand. Différents langages peuvent être utilisés pour écrire ce script, par exemple le langage "PERL" (marque déposée).

De façon pratique, la requête est habituellement affichée sur un écran informatique sous la forme d'un formulaire compris dans une page 25 "HTML". Le langage "HTML" permet de poster un formulaire à une adresse "URL". Le formulaire comporte un ou plusieurs champs, obligatoires ou non, qui sont remplis par un utilisateur à l'aide des moyens de saisie habituels : clavier pour le texte, souris pour les cases à cocher ou les boutons dits "radio", etc. Le contenu du formulaire (ainsi qu'éventuellement des 30 informations et instructions dites "cachées") est émis à destination du serveur "WEB". Le code "HTML" de la page décrit la structure matérielle du formulaire (cadre, graphisme, couleur, et tout autre attribut), ainsi que la

structure des champs de données à saisir (nom, longueur, type de données, etc.).

La transmission peut s'effectuer selon deux types de formats "HTTP" principaux. Un premier format utilise la méthode dite "POST" et un  
5 second la méthode dite "GET". Une information de type de format est présente dans le code de la page formulaire.

Ce mécanisme n'est cependant pas directement transposable à une carte à puce, même si celle-ci offre la fonctionnalité serveur "WEB" conformément à l'une des caractéristiques de l'invention.

10 On va maintenant décrire un exemple d'architecture permettant d'activer une application quelconque, de type conventionnel, via un serveur "WEB" sur la carte à puce, par référence à la figure 5.

Le serveur marchand 4 active une requête "HTTP" de type "GET" à une adresse "URL" qui peut se présenter de la façon suivante :

15 "http://@carte:8080/xxx.8080/cgi-bin/le\_cgi ? param1+param2"  
(4),

dans laquelle "@carte" est l'adresse "IP" du terminal supportant la carte à puce (par exemple l'adresse de rebouclage "127.0.01" de la relation (1)), "le-cgi" est un script "CGI" particulier à exécuter sur la carte à puce 8 et  
20 "param1" et param2" des paramètres à passer au script précité. La requête est tout d'abord transmise à l'enceinte sécurisée 6, via les nœuds de communication 50 et 60 (figure 3).

Une session s'établit entre le terminal et le lecteur de carte à puce. Ensuite une autre session s'établit entre une paire d'agents intelligents, 641  
25 et 841, localisés dans les couches spécifiques de l'enceinte sécurisée 6 et de la carte à puce 8, respectivement 64 et 84. Les données traversent alors le multiplexeur de paquets 640 de la couche protocolaire de communication spécifique 64. Elles traversent ensuite les couches protocolaires classiques (voir figure 2). Cependant, pour mieux mettre en évidence certains aspects  
30 spécifiques de l'invention, qui vont être explicités ci-après, ces couches sont divisées en deux parties sur la figure 5 : un gestionnaire d'ordres "APDU" 65a et des couches protocolaires basses 65b (normes ISO 7816-3).

De même, dans la carte à puce 8, elles traversent les couches protocolaires basses, référencées 85b, et le gestionnaire d'ordres "APDU" côté carte, référencé 85a, puis le multiplexeur de paquets 840, pour être reçues par l'agent intelligent 841, que l'on appellera "agent WEB".

5 Il convient de remarquer que les données adressées à l'agent "WEB" 841 sont transportées, de façon conventionnelle en soi, sous formes d'ordres "APDU" destinés à l'application particulière "Multiplexeur de paquets" 840. Le gestionnaire d'ordres "APDU" 85a sélectionne cette  
10 application de manière tout à fait similaire aux autres applications présentes dans la carte à puce 8,  $A_1$  à  $A_n$ . En d'autres termes, le multiplexeur de paquets 840 est vu par le gestionnaire d'ordres "APDU" 85a comme une application carte ordinaire.

La requête "HTTP" est alors analysée par l'agent "WEB" 841 qui détecte une référence à un répertoire particulier, que l'on appellera ci-après  
15 par convention "cgi-smart", d'une part, et à une application particulière, par exemple  $A_i$ . Le chemin complet est donc, en l'occurrence, "cgi-smart/ $A_i$ ".

Selon une caractéristique du procédé de l'invention, l'entité ci-dessus désigne un script particulier associé à une application également particulière.

20 Selon un autre aspect de l'invention, on implante dans la carte à puce 8 des agents intelligents particuliers, que l'on appellera ci-après "Agents traducteurs de script" ou de façon abrégée "ATS". Le script est alors interprété par un des agents intelligents. Cette traduction peut être réalisée de différentes manières :

- 25 a/ par l'agent "WEB" 841 lui-même, qui est doté dans ce cas d'une double capacité ;
- b/ par un agent script unique capable de traduire l'ensemble des scripts présents dans la carte à puce 8 ;
- c/ par un agent de script dédié que l'on appellera "ATSD" ci-après (un  
30 par script) ; ou
- d/ par un agent "APDU" 850a du gestionnaire d'ordres "APDU" 85a, qui est doté, dans ce cas, d'une double capacité.

## 25

L'agent "APDU" 850a est une composante de la couche gestionnaire d'ordres "APDU" 85a. Cette dernière est une couche capable de centraliser tous les ordres "APDU" émis et/ou reçus par le système, de sélectionner des applications, parmi  $A_1$  à  $A_n$ , mais également d'offrir une interface de type agent intelligent. Elle est donc capable, selon l'une des caractéristiques de l'invention de communiquer avec tous les agents intelligents (via des sessions), que ces agents soient localisés dans l'enceinte 6 ou la carte à puce 8.

Dans le cas c/ ci-dessus, une session est ouverte entre l'agent "WEB" 841 et l'un des agents "ATSD".

La figure 5 illustre un exemple d'architecture pour laquelle les agents traducteurs sont du type "ATSD". Ils sont référencés  $ATS_1$  à  $ATS_n$  et associés aux applications  $A_1$  à  $A_n$ . L'application sélectionnée étant supposée être l'application  $A_p$ , la session s'établit entre l'agent "WEB" 841 et l'agent  $ATS_p$ .

Un agent traducteur de script génère une suite d'ordres "APDU". Une session est ouverte entre l'agent traducteur, par exemple l'agent  $ATS_p$ , et l'agent "APDU" 850a. Les ordres sont alors émis vers l'agent "APDU" 850a. Le gestionnaire d'ordres "APDU" 85a sélectionne l'application "CGA"  $A_p$  et lui transmet les ordres "APDU", ordres traduits et donc conventionnels, qu'elle est en mesure de comprendre. Cette application est donc correctement activée, sans avoir à la modifier ou à la réécrire.

Les réponses de l'application  $A_p$  sont transmises au gestionnaire d'ordres "APDU" 85a, à l'agent "APDU" 850a, puis de nouveau à l'agent  $ATS_p$  (et de façon plus générale à l'agent traducteur de script).

Les différents cheminements sont représentés symboliquement sur la figure 5 par des traits pleins reliant les blocs fonctionnels, ou en pointillés à l'intérieur de ces blocs.

Pour fixer les idées et sans que cela soit limitatif de la portée de la présente invention, la technique d'adressage étant désormais définie dans

## 26

sa généralité, on va maintenant détailler ci-dessous divers routages possibles, que l'on appellera cas d'utilisation et que l'on référencera CU-*n* :

CU-1 : communication entre le serveur marchand 4 et la carte à puce 8.

5 Pour ce faire, une adresse "URL" conforme à (1) est utilisée. Dans ce cas, il n'est pas nécessaire d'utiliser le clavier 62. La requête, transmise via le réseau Internet *Ri*, arrive sur le nœud de communication 50. Celui-ci identifie le port associé à la carte à puce, c'est-à-dire le port 8080, qui est le même que celui de l'enceinte sécurisée 6. Le nœud de communication 50  
10 achemine la requête vers le nœud de communication 60. Dans tous les cas, quelle que soit l'adresse "URL", ce dernier achemine le paquet de données reçues vers la carte à puce 8, et plus précisément vers le serveur "HTTP" carte à puce 81, via le nœud de communication 80. En dernier lieu, celui-ci active l'une des applications de la carte à puce 8, par exemple l'application  
15 *A<sub>1</sub>*.

CU-2 : communication entre deux applications de la carte à puce 8.

Par exemple, l'application *A<sub>1</sub>* veut communiquer avec l'application *A<sub>n</sub>*. La requête émanant de l'application *A<sub>1</sub>* est acheminée par le serveur "HTTP" 81. De façon pratique, une session s'établit entre une paire  
20 d'agents intelligents locaux à la carte à puce 8, selon le schéma qui a été explicité en regard de la figure 4. Le nœud de communication 80 n'entre pas en jeu. Il n'y a pas d'adaptation de protocole de communication à prévoir.

CU-3 : communication entre une application carte et l'application marchande 41 dans le serveur 4.

25 Ce cas peut se produire, notamment, lorsque la carte à puce 8 a reçu une requête du serveur marchand 4 (cas CU-1). Une application locale à la carte à puce 8, par exemple l'application *A<sub>1</sub>*, peut être activée. Une action déterminée, commandée par la requête reçue, est alors réalisée à l'intérieur de la carte à puce, par exemple une action de type "CGI", par  
30 exécution d'un script ou tout processus équivalent. Cette action est réalisée sous la commande d'agents intelligents traducteurs de script, comme il a été explicité en regard de la figure 5.

En résultat, l'application  $A_1$  pose une requête destinée au serveur 4. Après examen de l'adresse "IP", le serveur "HTTP" 81 oriente la requête vers le nœud de communication 80. Il s'établit une session entre la carte à puce 8 et l'enceinte sécurisée 6, plus précisément entre les nœuds de communication 60 et 80, selon le schéma qui a été décrit en regard de la figure 4. De même, le nœud de communication 60, après examen de l'adresse "IP", transmet la requête au nœud de communication 50. Ce dernier, après examen de l'adresse "IP", transmet à son tour la requête, via le réseau Internet *RI*, vers sa destination finale, c'est-à-dire vers le serveur 4.

Le processus peut comporter plusieurs aller et retour entre la carte à puce 8 et le serveur 4, pendant le temps d'une transaction. Lorsque le processus est terminé (fin du "CGI" par exemple), la réponse de la carte à puce est transmise au serveur marchand 4, via notamment les nœuds successifs de communication 80, 60 et 50.

CU-4 : communication entre une "application carte" et une "application terminal".

A titre d'exemple, l'application  $A_1$  veut par exemple communiquer avec un gestionnaire d'impression (non représenté) du terminal et pose une requête en ce sens. Après examen de l'adresse "IP" et du numéro de port, le serveur "HTTP" 81 oriente la requête vers le nœud de communication 80. La requête suit alors le même chemin que dans le cas CU-3, jusqu'à ce qu'elle atteigne le nœud de communication 50. Ce dernier, après examen de l'adresse "IP" et du numéro de port, oriente la requête vers l'application terminal adressée, par exemple le gestionnaire d'impression.

CU-5. : communication entre une "application carte" et une ressource de l'enceinte sécurisée.

On suppose tout d'abord, dans ce cas d'utilisation, que la carte à puce 8 est en mode "esclave" par rapport au serveur marchand 4 et que celui-ci a émis une requête à destination de la carte à puce 8. Cette requête est traitée de la façon explicitée par les cas CU-1 et CU-3. Il s'exécute par exemple un "CGI marchand" à l'intérieur de la carte à puce 8, de la manière

qui a été décrite en regard de la figure 5. Ce script s'exécute en activant l'une des applications, par exemple  $A_i$ , à l'aide d'un des agents traducteurs de script, par exemple  $ATS_i$ . On suppose que le CGI marchand a besoin d'informations en provenance du clavier 62 (mot de passe par exemple) ou  
5 d'autres informations d'authentification (en provenance d'un dispositif biométrique constituant l'une des ressources 63). Le CGI en question doit être exécuté avec un adressage "URL" particulier. L'application  $A_i$  émet une requête dont l'adresse est par exemple celle donnée par (2) ci-dessus. La présence du suffixe "/kb" indique au nœud de communication 60 qu'il faut  
10 reboucler la requête vers le serveur "HTTP" 61 qui à son tour active le gestionnaire 620 de clavier 62, et récupère les informations attendues (saisie d'un mot de passe par exemple). La réponse de la requête est transmise, par le même chemin, mais en sens inverse vers la carte à puce 8.

15 La réponse de la requête du serveur marchand 4 est alors retransmise à celui-ci. Un dialogue à plusieurs temps peut s'instaurer de manière similaire au cas CU-3.

Plusieurs CGI peuvent être exécutés pendant le temps d'une transaction.

20 Pour fixer les idées, un premier "CGI marchand" peut avoir pour résultat l'affichage sur un écran compris dans l'enceinte sécurisée 6 (l'une des ressources représentées sous la référence unique 63) d'un message invitant un utilisateur à composer un code et affichant un montant. Un deuxième CGI lit par exemple des informations transmises par le clavier 62.  
25 Un troisième CGI peut avoir pour résultat sur ce même organe de visualisation d'un message du type "CODE CORRECT" ou tout message similaire.

CU-6 : communication entre le terminal et une des ressources de l'enceinte sécurisée.

30 A titre d'exemple, une application du terminal 5 (dans sa partie non sécurisée), par exemple le navigateur "WEB" 51, désire communiquer avec l'une des ressources sécurisées, par exemple avec le clavier 62, et émet



une requête en ce sens. Le nœud de communication 50 examine l'adresse "URL", identifie le numéro de port de l'enceinte sécurisée 6 et transmet la requête à celle-ci. Le nœud de communication 60, du fait de sa programmation, oriente systématiquement les requêtes reçues, même si  
5 elles sont destinées à l'une des ressources internes à l'enceinte sécurisée 6, vers la carte à puce 8. A partir de ce stade, la requête suit un chemin similaire au cas CU-1. C'est la carte à puce 8 qui détermine s'il y lieu de retransmettre la requête vers la ressource sécurisée initialement adressée, éventuellement en la modifiant. La décision peut être le résultat d'une  
10 procédure d'identification mettant en jeu l'examen de données de sécurité enregistrées dans la carte à puce, notamment dans une mémoire de type à lecture seule, éventuellement sous forme chiffrée. Comme dans le cas CU-4, un élément externe à l'enceinte sécurisée 6 n'a donc jamais accès directement aux ressources sécurisées.

15 Cette dernière caractéristique permet des mises à jour de logiciels résidents dans l'enceinte sécurisée 6, des ajouts de logiciels ou des suppressions, au moins partielles, de ces logiciels, de façon plus fiable que dans l'art connu. En effet, il est d'usage d'authentifier des modifications de cette nature à partir d'une clé enfouie dans le logiciel de l'enceinte  
20 sécurisée 6.

Puisque seule la carte à puce 8 peut accéder de l'extérieur aux ressources protégées de l'enceinte sécurisée 6, le téléchargement de ressources logicielles peut donc s'effectuer à partir d'un serveur Internet, par l'intermédiaire de la carte à puce, tout en conservant un très grand  
25 degré de sécurité. Il suffit que les données téléchargées, si elles sont sensibles, soient convenablement chiffrées, en faisant usage d'un algorithme robuste et/ou d'une clé de chiffrement suffisamment longue. Du fait de la fonction d'intermédiaire jouée par la carte à puce 8, le mécanisme mis en œuvre dans l'invention est *a priori* plus fort que celui d'un simple enfouissement de clé dans un organe de mémoire (non représenté) de  
30 l'enceinte sécurisée 6.

On peut également modifier le contenu des ressources logicielles de l'enceinte sécurisée 6 directement à partir d'une carte à puce 8, en téléchargeant des pièces de logiciel enregistrées dans celle-ci. Le volume de logiciel ainsi téléchargé est cependant limité par les ressources propres  
5 de la carte à puce (capacité de mémoire), ce qui n'est pas le cas *a priori* d'un téléchargement par réseau Internet à partir d'un serveur "WEB", le serveur pouvant être doté de ressources informatiques importantes. Le temps de téléchargement est naturellement dépendant de la quantité de logiciel à télécharger, mais l'utilisation de modems rapides et/ou de lignes  
10 de communication à haut débit est de nature à maintenir ce temps dans des limites tout à fait raisonnables pour les applications envisagées.

A la lecture de ce qui précède, on constate aisément que l'invention atteint bien les buts qu'elle s'est fixés.

Elle permet notamment, tout en conservant la possibilité d'utiliser  
15 des composants classiques et des modes de communication normalisés, notamment entre l'enceinte sécurisée et la carte à puce, via le lecteur, un adressage et des communications compatibles avec le protocole Internet "HTTP". Elle transforme la carte à puce en serveur-client "WEB", capable d'effectuer des opérations de type "CGI". Elle permet notamment un  
20 adressage direct et interactif de la carte à puce, à partir d'un serveur "WEB", via le réseau Internet, ou en sens contraire. Elle ne nécessite aucune application spécifique marchande sur le terminal lui-même et sur l'enceinte sécurisée. Elle offre une très grande souplesse et s'adapte aisément à de nombreux domaines d'application. Elle n'entraîne que des  
25 modifications mineures des composants utilisés, modifications qui se résument essentiellement à l'implantation de pièces de logiciel spécifiques, étant entendu que le mot "spécifique" n'indique pas une dépendance vis-à-vis des applications traitées. Notamment les applications résidentes dans la carte à puce restent des applications standards et ne nécessitent aucune  
30 réécriture. En outre, les applications spécifiques, d'un point de vue "application marchandes" sont entièrement localisées dans le serveur "WEB" éloigné. Ce dernier peut en contenir une pluralité. La mise à jour, la

suppression de ces applications, ainsi que l'ajout de nouvelles applications, sont de ce fait aisés. Cette caractéristique offre une grande flexibilité. La version des programmes est identique pour tous les terminaux qui se connectent sur le serveur. Enfin, la sécurité assurée par l'invention est très grande. On peut faire appel à des algorithmes de chiffage robustes et des clés de grande longueur pour les communications sur le réseau Internet. En outre, selon une caractéristique de l'invention, toutes les requêtes provenant de l'extérieur de l'enceinte sécurisée, que ce soit de la partie non sécurisée du terminal ou directement du réseau Internet, doivent obligatoirement passer par la carte à puce et restent sous son contrôle exclusif. Celle-ci décide seule, en fonction, par exemple, de données de sécurité résidentes, de l'usage qui doit être fait de ces requêtes. Or la carte à puce reste la propriété du porteur.

Il doit être clair cependant que l'invention n'est pas limitée aux seuls exemples de réalisations explicitement décrits, notamment en relation avec les figures 3 à 5.

Dans un mode de réalisation (non représenté) l'enceinte sécurisée pourrait ne contenir qu'un lecteur de carte à puce, la ou les application(s) enregistrée(s) dans la carte à puce étant autosuffisante(s) pour authentifier le porteur et/ou permettre une transaction entre le serveur "WEB" éloigné et la carte à puce. Le clavier peut être omis et remplacé par l'une des ressources sécurisées, tel qu'un dispositif biométrique. Enfin, on peut adjoindre au premier lecteur de carte à puce un deuxième lecteur de carte à puce, voire plusieurs.

### REVENDICATIONS

1. Terminal muni d'une enceinte sécurisée destinée à communiquer avec au moins un serveur de type "WEB", via un réseau de type Internet, selon un premier protocole de communication de type Internet, ladite enceinte sécurisée comprenant au moins un lecteur de carte à puce, ladite carte à puce stockant au moins une application logicielle, caractérisé en ce que ledit terminal (5) comprend une partie non sécurisée comprenant au moins un premier module dit premier nœud de communication (50), ladite enceinte sécurisée (6) comprend au moins un deuxième module dit deuxième nœud de communication (60) et ladite carte à puce (8) comprend au moins un troisième module dit troisième nœud de communication (80), en ce que lesdits nœuds de communication (50, 60, 80) comprennent des première, deuxième et troisième piles protocolaires, respectivement, comprenant chacune un nombre déterminé de couches logicielles de communication dites standards et des première, deuxième et troisième pièces de logiciel spécifique (64, 84), respectivement, comprenant chacune au moins une première entité logicielle (641, 841), lesdites premières entités logicielles étant appariées deux à deux, en ce que ledit premier nœud (50) autorise au moins des communications entre ledit terminal (5) et ledit serveur "WEB" (4), selon ledit premier protocole de communication de type Internet, en ce que lesdites premières entités desdites première et deuxième pièces de logiciel spécifique autorisent l'établissement d'une session d'échanges de données bilatéraux entre ledit terminal (5) et la dite enceinte sécurisée (6), selon un deuxième protocole de communication déterminé, en ce que lesdites premières entités (641, 841) desdites deuxième (64) et troisième (84) pièces de logiciel spécifique autorisent au moins l'établissement d'une session d'échanges de données bilatéraux entre la dite enceinte sécurisée (6) et ladite carte à puce (8), via ledit lecteur de carte à puce, selon un troisième protocole

de communication déterminé, de manière à pouvoir mettre en relation au moins une desdites applications logicielles ( $A_1-A_n$ ) de la carte à puce (8) avec ledit serveur de type "WEB" (4).

5       2. Terminal selon la revendication 1, caractérisé en ce que lesdites premières entités appariées sont constituées de modules logiciels, dits agents intelligents (641, 841), établissant lesdites sessions.

10       3. Terminal selon la revendication 1, caractérisé en ce qu'il comprend, dans ladite partie non sécurisée, au moins une application constituée par un navigateur de type "WEB" (51), en ce que ledit premier protocole de type Internet est le protocole "HTTP/TCP-IP" comporte un adressage de type dit "URL", comprenant un élément d'adresse Internet dite "IP" et un  
15       numéro de port, pour la sélection dudit terminal (5) et d'un élément interne à ce terminal (5), en ce que ladite première entité de ladite pièce de logiciel spécifique dudit premier nœud de communication (50) identifie ledit élément d'adresse "IP" et ledit numéro de port, en ce que, en résultat de ladite identification, des données reçues dudit serveur de type "WEB" (4) sont aiguillées vers ledit navigateur de type "WEB" (51), selon ledit premier protocole de type Internet, ou traduites et transmises vers  
20       ledit deuxième nœud de communication (60), selon ledit deuxième protocole de communication déterminé, dans un premier sens de transmission de données, et en ce que sur ladite identification, des données reçues du deuxième nœud de communication (60), sont aiguillées vers ledit navigateur de type "WEB" (51) ou vers ledit serveur de type "WEB" (4), selon ledit premier protocole de type Internet, dans un  
25       second sens de transmission de données.

30       4. Terminal selon la revendication 3, caractérisé en ce que ladite enceinte sécurisée (6) comprend en outre au moins un clavier de saisie de données (62) et au moins un serveur "HTTP" dit d'enceinte (61) disposé entre ledit clavier (62) et le dit deuxième nœud de communication (60), en ce que ladite première entité (641) de ladite

pièce de logiciel spécifique (64) dudit deuxième nœud de communication (60) identifie ledit élément d'adresse "IP" et ledit numéro de port, en ce que des données reçues dudit premier nœud de communication (50) sont traduites et toujours transmises vers ledit troisième nœud de communication (80), selon ledit troisième protocole de communication déterminé, dans un premier sens de transmission de données, et en ce que sur ladite identification, des données reçues du troisième nœud de communication (80), sont aiguillées vers ledit serveur "HTTP" (61) ou traduites et transmises vers ledit premier nœud de communication (50), selon ledit deuxième protocole déterminé, dans un second sens de transmission de données.

5. Terminal selon la revendication 4, caractérisé en ce que ladite enceinte sécurisée comprend au moins une ressource informatique supplémentaire (63) connectée audit serveur "HTTP" (61) de l'enceinte sécurisée (6), et en ce que ladite adresse de type "URL" comprenant un élément supplémentaire, ledit serveur "HTTP" (61) sélectionne, sur identification dudit élément d'adresse supplémentaire, ledit clavier (62) ou l'une desdites ressources informatiques supplémentaires (63).

6. Terminal selon la revendication 5, caractérisé en ce que ladite ressource informatique supplémentaire (63) est un dispositif d'authentification biométrique.

7. Terminal selon la revendication 4, caractérisé en ce que ladite carte à puce stocke plusieurs applications logicielles ( $A_1-A_n$ ), en ce qu'elle comprend un serveur "HTTP" dit de carte (81) disposé entre lesdites applications logicielles ( $A_1-A_n$ ) et ledit troisième nœud (80), et en ce que ledit serveur "HTTP" de carte (81) active sélectivement au moins l'une desdites applications logicielles ( $A_1-A_n$ ) sur réception d'une requête en provenance dudit deuxième nœud (60) ou transmet les requêtes émises par lesdites applications ( $A_1-A_n$ ) vers ledit troisième nœud de communication (80).

8. Terminal selon la revendication 7, caractérisé en ce que ladite carte à puce (8) comprend en outre une deuxième entité logicielle ( $ATS_1-ATS_i$ ) apte à interpréter une suite d'instructions véhiculées par lesdites données reçues dudit troisième nœud de communication (80), et à la traduire en une suite d'ordres, ladite deuxième entité logicielle ( $ATS_1-ATS_i$ ) coopérant avec lesdites applications logicielles ( $A_1-A_n$ ) et ladite pièce de logicielle spécifique (84) dudit troisième nœud de communication (80), ladite suite d'instructions traduite étant associée à une desdites applications logicielles à activer ( $A_1-A_n$ ) de ladite carte à puce (8).

9. Terminal selon la revendication 8, caractérisé en ce que ladite suite d'instructions à interpréter étant constituée par un script, chacune desdites deuxième entités logicielles est constituée par un module logiciel dit agent intelligent traducteur de script ( $ATS_1-ATS_i$ ).

10. Terminal selon la revendication 1, caractérisé en ce que ledit serveur de type "WEB" (40) stocke une application logicielle dite marchande (41) destinée à être mise en communication interactive avec au moins l'une desdites applications logicielles ( $A_1-A_n$ ) de ladite carte à puce (8) au travers desdits premier (50), deuxième (60) et troisième nœuds (80) de communication.

**THIS PAGE BLANK (USPTO)**



FIG.1  
ART ANTERIEUR

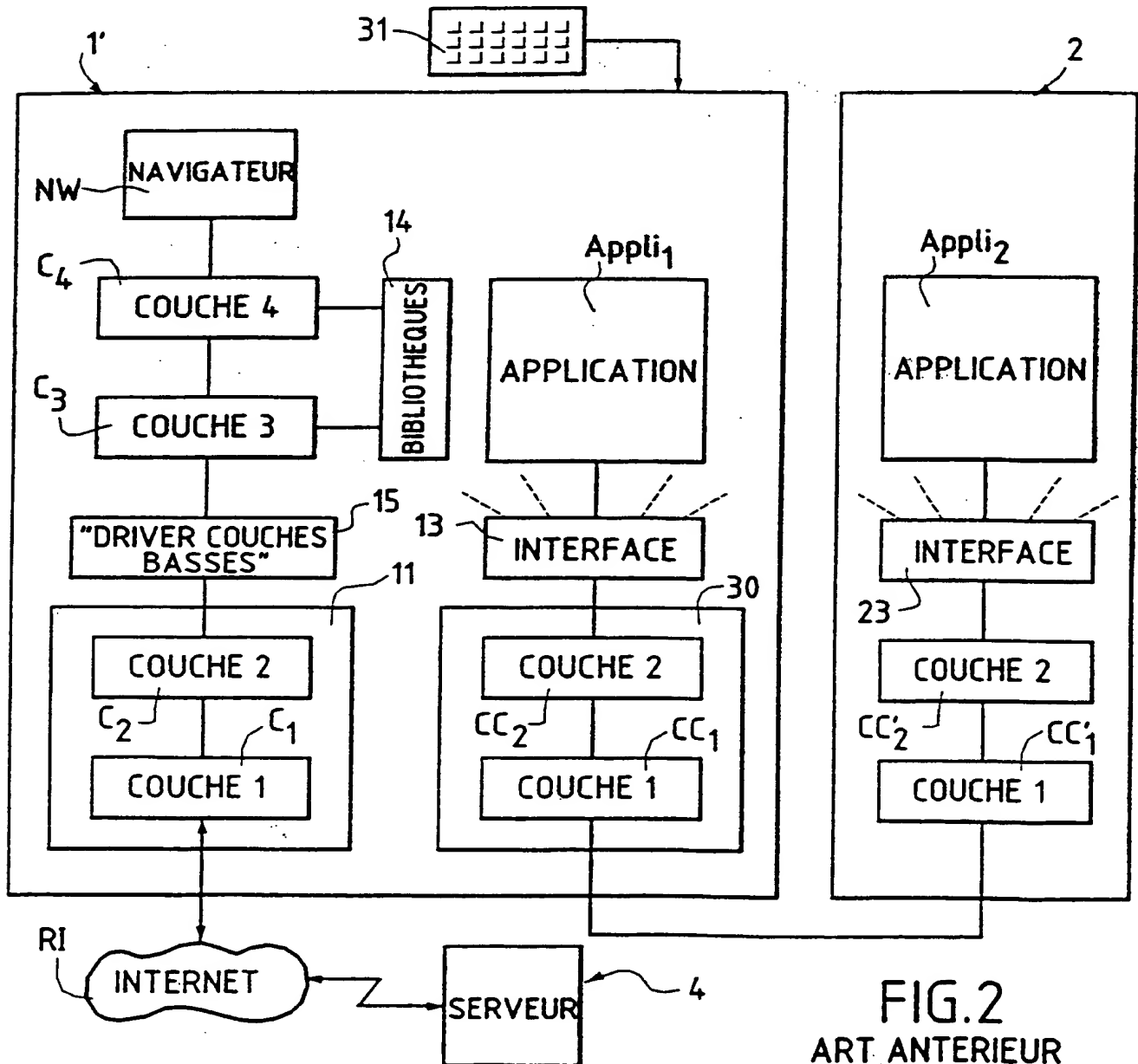
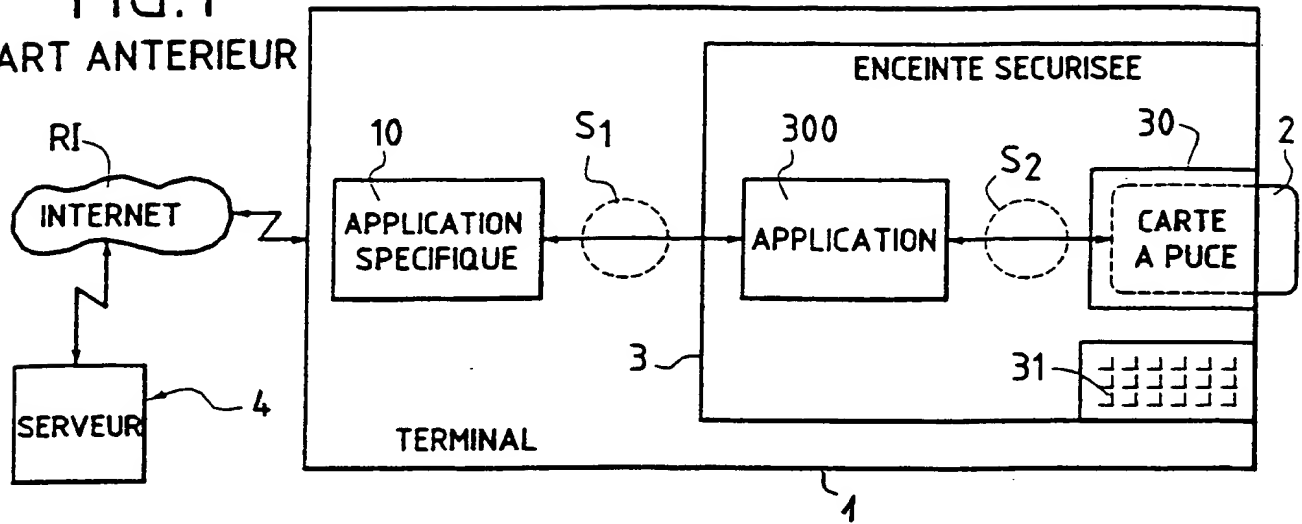
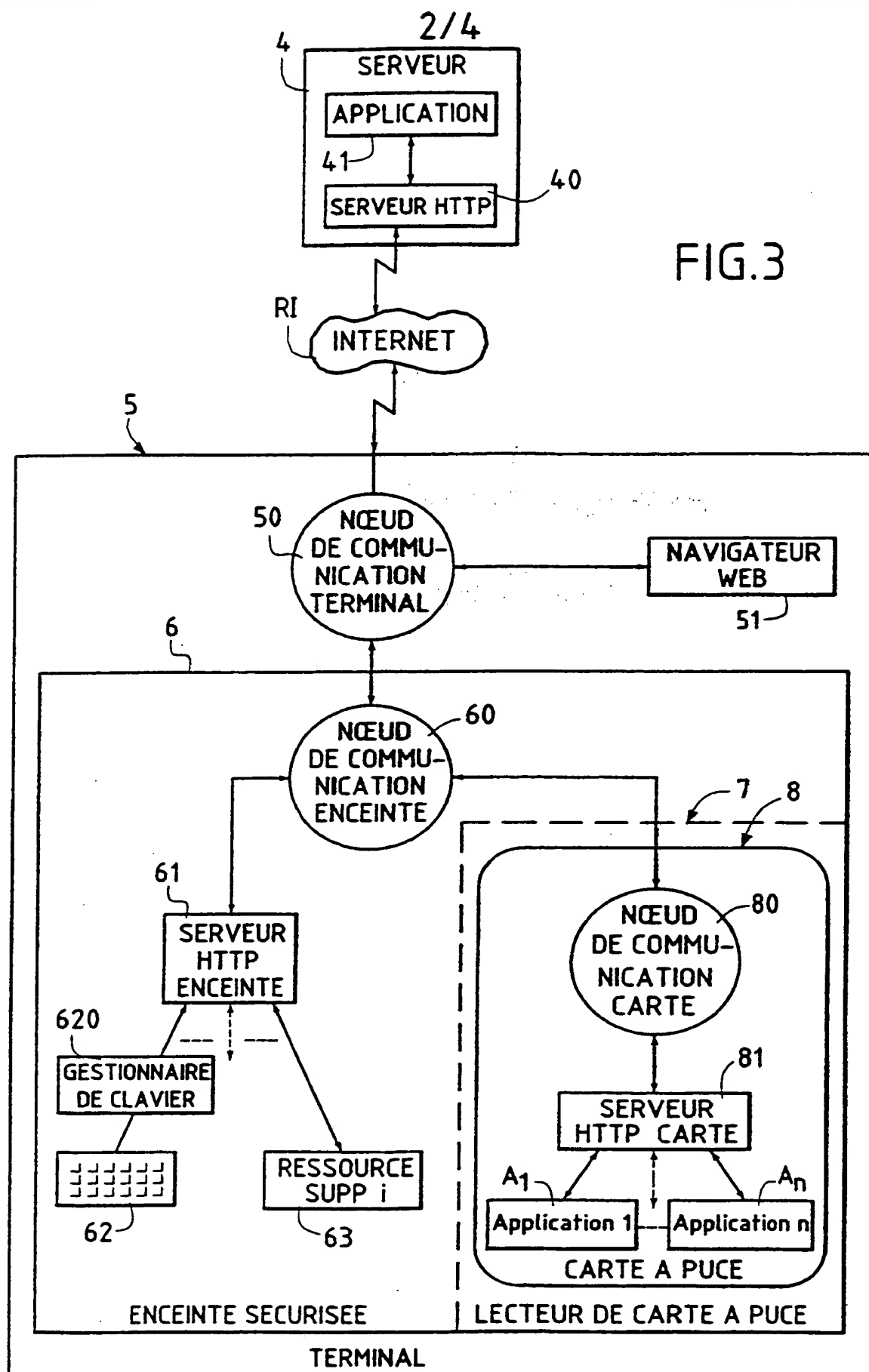


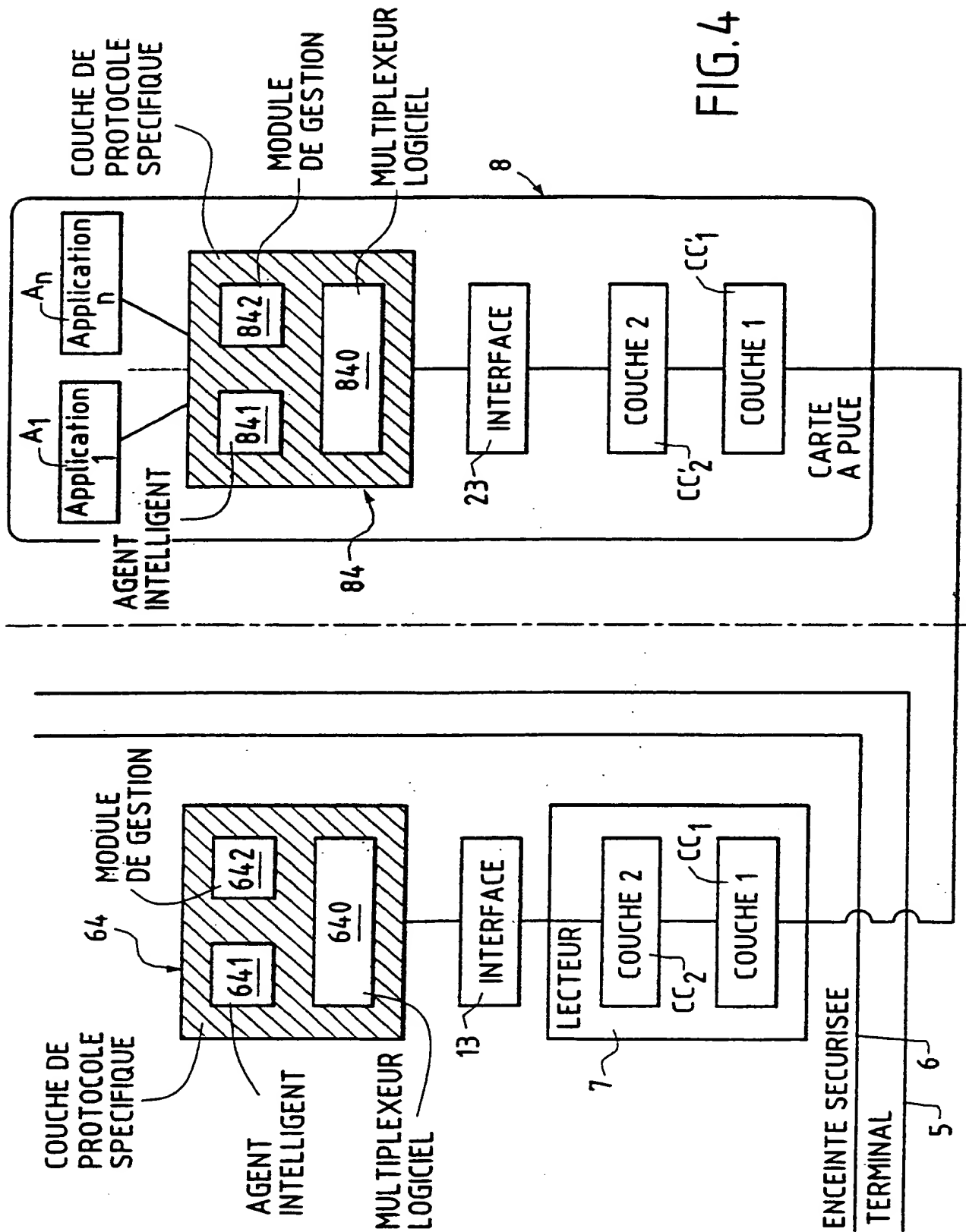
FIG.2  
ART ANTERIEUR

**THIS PAGE BLANK (USPTO)**

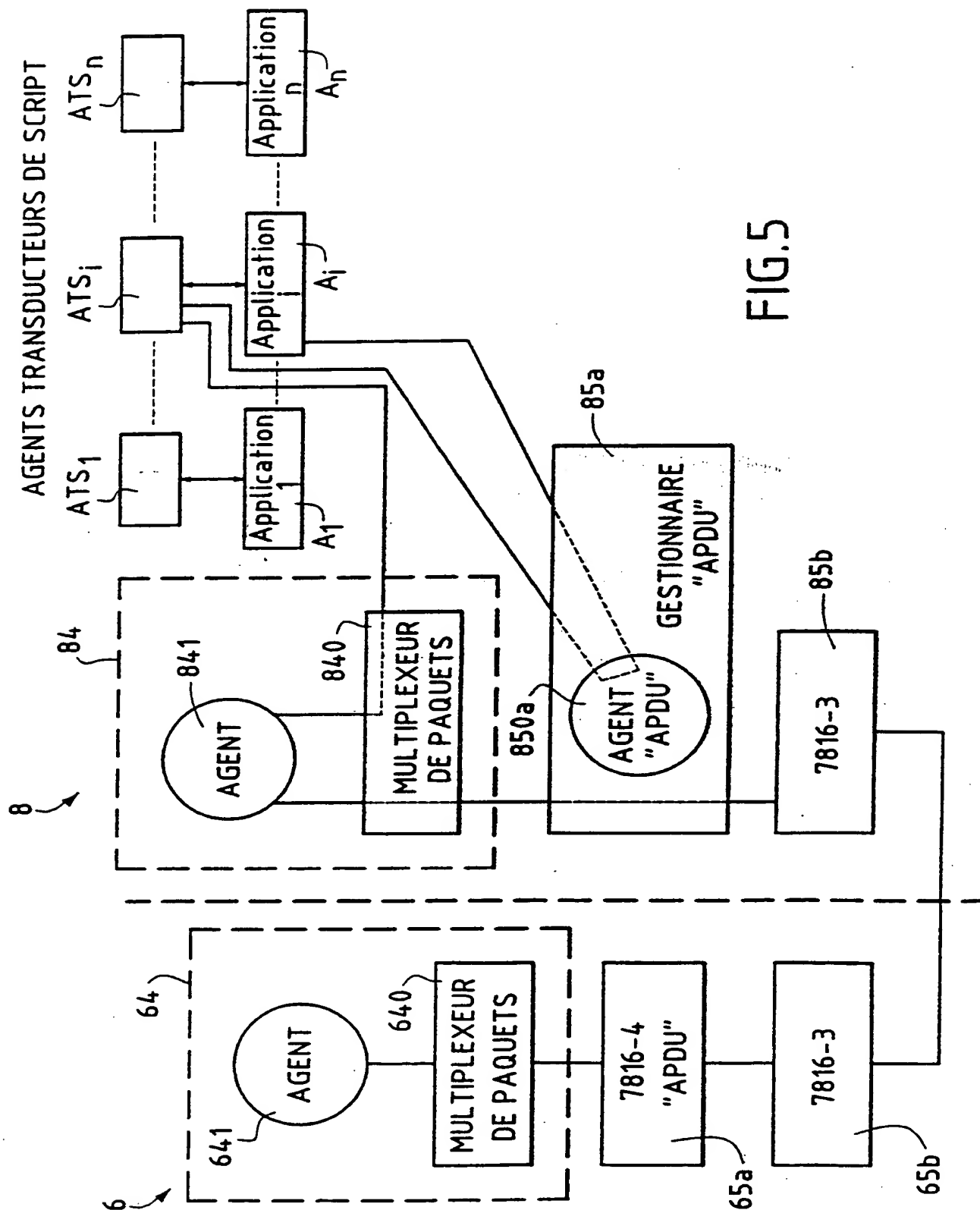


**THIS PAGE BLANK (USPTO)**

3/4



**THIS PAGE BLANK (USPTO)**



**THIS PAGE BLANK (USPTO)**



# INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 00/02979

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 57474 A (GEMPLUS CARD INT ;MARTINEAU PHILIPPE (FR); MERRIEN LIONEL (US); SI) 17 December 1998 (1998-12-17) page 8, line 25 -page 11, line 10 page 14, line 12-25 page 16, line 6 -page 18, line 25 figure 2	1-10
A	WO 97 50207 A (TELIA AB PUBL) 31 December 1997 (1997-12-31) page 2, line 17 -page 4, line 6 page 8, line 9-15 page 9, line 16 -page 10, line 1	1-10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

\* Special categories of cited documents :

\*A\* document defining the general state of the art which is not considered to be of particular relevance

\*E\* earlier document but published on or after the international filing date

\*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

\*O\* document referring to an oral disclosure, use, exhibition or other means

\*P\* document published prior to the international filing date but later than the priority date claimed

\*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

\*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

\*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

\*Z\* document member of the same patent family

Date of the actual completion of the international search

30 March 2001

Date of mailing of the international search report

06/04/2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Lázaro, M.L.

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 00/02979

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9857474 A	17-12-1998	AU 8113798 A CN 1284230 T EP 1050145 A TW 378308 B ZA 9805151 A	30-12-1998 14-02-2001 08-11-2000 01-01-2000 13-04-1999
WO 9750207 A	31-12-1997	SE 509033 C EP 0906680 A NO 985951 A SE 9602528 A	30-11-1998 07-04-1999 24-02-1999 27-12-1997

# RAPPORT DE RECHERCHE INTERNATIONALE

D Inde Internationale No

PCT/FR 00/02979

**A. CLASSEMENT DE L'OBJET DE LA DEMANDE**  
CIB 7 H04L29/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

**B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE**

Documentation minimale consultée (système de classification suivi des symboles de classement)  
CIB 7 H04L G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)  
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

**C. DOCUMENTS CONSIDERES COMME PERTINENTS**

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 98 57474 A (GEMPLUS CARD INT ;MARTINEAU PHILIPPE (FR); MERRIEN LIONEL (US); SI) 17 décembre 1998 (1998-12-17) page 8, ligne 25 -page 11, ligne 10 page 14, ligne 12-25 page 16, ligne 6 -page 18, ligne 25 figure 2	1-10
A	WO 97 50207 A (TELIA AB PUBL) 31 décembre 1997 (1997-12-31) page 2, ligne 17 -page 4, ligne 6 page 8, ligne 9-15 page 9, ligne 16 -page 10, ligne 1	1-10

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

\* Catégories spéciales de documents cités:

- \*A\* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- \*E\* document antérieur, mais publié à la date de dépôt international ou après cette date
- \*L\* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- \*O\* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- \*P\* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- \*T\* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- \*X\* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- \*Y\* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- \*G\* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

30 mars 2001

Date d'expédition du présent rapport de recherche internationale

06/04/2001

Nom et adresse postale de l'administration chargée de la recherche internationale  
Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel (+31-70) 340-2040, Tx. 31 651 epo nl.  
Fax (+31-70) 340-3016

Fonctionnaire autorisé

Lázaro, M.L.

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Numéro de l'acte internationale No

PCT/FR 00/02979

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9857474 A	17-12-1998	AU 8113798 A	30-12-1998
		CN 1284230 T	14-02-2001
		EP 1050145 A	08-11-2000
		TW 378308 B	01-01-2000
		ZA 9805151 A	13-04-1999
WO 9750207 A	31-12-1997	SE 509033 C	30-11-1998
		EP 0906680 A	07-04-1999
		NO 985951 A	24-02-1999
		SE 9602528 A	27-12-1997